Escola Politècnica Superior
de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

TRABAJO DE FIN DE CARRERA

TÍTULO: Análisis de la seguridad en IP/MPLS VPN: comparación con ATM

TITULACIÓN: Ingeniería Técnica de Telecomunicaciones, especialidad Telemática

AUTOR: Luis de Diego Morcillo

CODIRECTOR: J. Manuel Yúfera Gómez

FECHA: 5 de Septiembre 2005

Título: Análisis de la seguridad de IP/MPLS VPN: comparación con ATM

Autor: Luis de Diego Morcillo

Codirector: J. Manuel Yúfera Gómez

Fecha: 5 de Septiembre de 2005

Resumen

La evolución de las redes *backbones* a mediados de los '90 supuso el primer gran paso hacia la Internet del siglo XXI: una red común para todos los servicios y aplicaciones. Este es uno de los sueños de los defensores de las redes IP, y de "la red única". Y que supuso pasar de ATM, una tecnología sólida y muy consolidada en las redes de los proveedores, a una tecnología de etiquetaje denominada MPLS, que debía aportar más velocidad y mayor versatilidad.

Este TFC nace de la duda de las grandes compañías de servicios y de los grandes clientes, de la seguridad de una arquitectura de red que surge con la idea de sustituir ATM. Durante años, ATM les había proporcionado niveles de velocidad, robustez y seguridad que superaban anteriores soluciones.

Las grandes compañías necesitan estar seguras de que la información que transmiten de una compañía a otra o a sus propias sucursales, no corre peligro. ATM, en este aspecto les aportaba eso que añoraban en décadas anteriores, y la idea de cambiar de ATM a una tecnología basada en IP, no convencía a nadie. Como se podrá observar, es uno de los principales puntos de investigación para todos aquellos que han optado por MPLS en detrimento de ATM.

Durante las primeras páginas se atacará el tema de la seguridad en nuestras redes, para tener una visión más directa de los peligros de los que deben defenderse ATM y MPLS.
Durante los siguientes puntos, y como principal objetivo de este TFC, se explicaran las soluciones que se adoptan para que las grandes redes de proveedores no sucumban frente a los ataques de los *hackers*. Con ello también, todas las opciones que se barajan para encontrar una solución lo más cercana posible a las exigencias de los grandes clientes, y abrir el camino a nuevas tecnologías que seguro en un futuro no muy lejano invadirán las *backbones*.

Title: Analysis of IP/MPLS VPN security: comparison to ATM

Author: Luis de Diego Morcillo

Codirector: J. Manuel Yúfera Gómez

Date: September, 5th 2005

Overview

The evolution of the networks backbones in the middle of the ' 90 supposed the first great step towards the Internet of century XXI: a common network for all the services and applications. This is one dream of the IP network defenders' and of "the unique network" too. That supposed to pass from ATM, a solid technology and very consolidated in the networks of the providers, to a labeled technology called MPLS, which had to contribute with more speed and greater changeableness.

This TFC born from the doubt of great service providers and great customers, from the network architecture security that appears with the idea of replace ATM. During years, ATM had provided to them speed levels, robustness and security that exceeded previous solutions.

Great customers need to be sure that the information that they transmit from a company to another one, or their own sites, is not in danger. ATM, in this aspect, contributed with this aspect, and the idea to change ATM to a technology based on IP did not convince anybody. As it will be possible observed, it's one of the main points of investigation for all those that have decided on MPLS in ATM damage.

During early pages will be attacked the subject of the security in our networks, in order to have a better direct vision of the dangers of which ATM and MPLS must be defended. During the following points, and like main objective of this TFC, it is going to explain the solutions that are adopted so that great provider's networks do not succumb as opposed to the attacks of hackers. With it also, all the options that are shuffled to find the nearest possible solution to the customers' demands, and it will open the way to new technologies that surely will invade backbones in a future not very distant.

Me gustaría dedicar este trabajo a todas las personas
que me han aguantado durante los últimos 6 meses,
pero en especial a mi familia, y a Carol
por mostrarme la luz en la oscuridad de Milano

ÍNDICE

INTRODUCCIÓN

Vivimos en una era de continuos cambios, dónde lo que ayer era sofisticado y una tecnología puntera, mañana será una reliquia del pasado. Año tras año se desarrollan nuevos protocolos, un sinfín de aplicaciones nuevas, ideas, proyectos, etc.

Esto se cumple inevitablemente en el variado pero complejo mundo de las telecomunicaciones. Y en este aspecto, la atención por parte de los operadores se focaliza actualmente en poder ofrecer cada vez una gama más extensa de servicios adecuándolos a la "Calidad de Servicio" (*QoS*). Dentro de este contexto, podemos encontrar uno de los retos más deseados por las grandes compañías de servicios y por las grandes operadoras de redes: la integración de los servicios en una *única* plataforma. Con la ISDN (*Integrated Services Digital Networks*) se dio el primer paso hacia esta integración, aunque sólo a nivel de acceso, entre servicios de voz (telefonía) y transmisiones de datos. En esa dirección, entre finales de los '80 y principio de los '90, se desarrolló ATM (*Asynchronous Transfer Mode*) como primera tentativa seria de crear un estándar universal para redes multiservicio (más información al respecto en el Anexo C).

En la actualidad, MPLS constituye un escalón fundamental para una mejor escalabilidad y eficiencia; siendo considerado indispensable para los nuevos cimientos de la Internet del siglo XXI. Aunque MPLS es relativamente joven, ya ha estado implementado con éxito en las redes de los mayores ISPs mundiales, que han utilizado su funcionalidad para ofrecer servicios de Red Privada Virtual (RPV - VPN) y para el transporte del tráfico telefónico comercial. De esta manera, progresivamente han ido substituyendo sus antiguas redes centrales basadas en IP/ATM hacía una backbone IP/MPLS.

Este trabajo, surge de la duda de muchos de los grandes clientes, que no confían en una tecnología que trabaja en el nivel 3 de OSI. Entienden que una tecnología que trabaja a este nivel nunca puede ser segura. Por lo tanto, el objetivo principal de este trabajo es descubrir si MPLS es tan insegura como creen sus detractores, o sólo se trata de miedo al cambio.

El primer capítulo de este TFC servirá para conocer qué es la seguridad y las grandes amazas que existen hoy en día. De esta manera, se podrá atacar mejor los dos temas que analizan la seguridad en ATM y MPLS. En ellos, se podrán observar las vulnerabilidades y las soluciones adoptadas para contrarrestarlas. Estas soluciones irán acorde con la tecnología utilizada y los elementos que se utilizan, y por lo tanto se añadirán pequeños comentarios sobre su correspondencia con otras tecnologías. Porque no existe ninguna tecnología que sea perfecta, segura. Como veremos pues, incluso ATM tiene problemas de seguridad, y su reto, como el del resto de tecnologías, es intentar tapar los agujeros que deja su diseño.

Con ello, llegaremos al último punto dónde se expondrán las conclusiones de un trabajo que se extiende más allá de las páginas de los capítulos. Aunque, posiblemente antes de leerlas, la pregunta: ¿Es MPLS tan seguro como ATM?; ya habrá sido contestada.

CAPÍTULO 1. LA SEGURIDAD EN NUESTRAS REDES

Sin lugar a dudas, la seguridad es uno de los temas que más importa a las grandes empresas, y por el contrario, poco estudiado en los libros de redes. Tal vez, la gran eclosión de las amenazas existentes en Internet (gusanos, el spyware, etc.) ha hecho que los autores incluyan en sus libros un capítulo sobre este tema. Y ese inconformismo y miedo de las grandes empresas es una de las razones de ser de este trabajo.

Durante este capítulo, antesala de la comparación entre las dos tecnologías, podremos descubrir qué es la seguridad, algunas de las herramientas que hay para consérvala y las grandes amenazas de nuestras redes. De esta manera, comprenderemos hasta qué punto es importante que las empresas y los usuarios se preocupen de la seguridad. También, será útil para entender mejor las amenazas y contramedidas que se verán durante los dos próximos capítulos.

1.1. ¿Que es la seguridad?

Esta es una de aquellas palabras que ha perseguido a la humanidad desde sus inicios. Desde que el hombre es hombre, ha tenido que resguardarse de los peligros que les suponía vivir en la naturaleza, afrontar el miedo a que extranjeros invadan sus tierras, o que ladrones les roben mientras pasean por la calle.

La seguridad es una palabra que engloba muchas situaciones en la vida: el amor, el dinero, la salud, etc. Pero todas ellas pueden ser afrontadas en mayor o menor medida según lo vulnerables que son los atacados y lo preparados que estén para contrarrestar el ataque.

La manera de resguardarse de los ataques ha ido evolucionando según las necesidades del hombre: desde tener encendida una hoguera para espantar los animales, a construir grandes fortificaciones para repeler los ataques de los enemigos o crear sprays de autodefensa.

Ni el mundo empresarial, ni el mundo de las telecomunicaciones está exento de los peligros de los “chicos malos” (como los llama Kurose y Ross en su libro “Redes de Computadores. Un enfoque descendente basado en Internet”). Tanto las grandes empresas interconectadas con sedes a miles de quilómetros de distancia, como los simple usuarios de Internet, son como un delicioso pastelito para los “chicos malos”

Internet es muy insegura; una encuesta de la FBI en el año 2002 lo demuestra. En ese año el 90% de los encuestados (grandes empresas y agencias del gobierno) detectaron intrusiones en la seguridad informática en el último año, y el 80% reconoció como consecuencia pérdidas financieras.

Año tras año, el número de virus y gusanos que se cuelan en nuestros sistemas va en aumento, e incluso los ataques han ido modificando su disfraz. Por eso desde hace poco podemos hablar de *spyware* y de *troyanos*, además de los ya conocidos virus y gusanos. Por ello son muchas las empresas que han sacado al mercado productos de defensa: antivirus, antisyware, antitroyanos, etc. Todos dedicados, junto con otros sistemas de defensa, a preservar la seguridad de los usuarios de la red y a reducir el número de vulnerabilidades.

1.1.1. Servicios para la seguridad

Los "chicos malos" obtienen la información de las comunicaciones de los usuarios. La falta de seguridad de estas comunicaciones, propicia la obtención de contraseñas en texto en claro, direcciones de redes, puertos, etc. Con toda esta información, los atacantes-intrusos pueden conseguir entrar en la red, enviar mensajes en nombre de otros y muchas otras formas de atacar.

Existen muchas maneras de conseguir información de otras personas, aunque también existen sistemas para evitar que se produzcan esos robos de información. Para preservar la seguridad de las comunicaciones y de las redes privadas, existen una serie de servicios a tener en cuenta:

- Confidencialidad: Es la protección de la información transmitida, de tal manera que sólo el emisor y el receptor deseado entiendan el contenido del mensaje. Por ello, la información es encriptada (transformada-disfrazada) para que el mensaje interceptado por una tercera persona no pueda ser desencriptado y por lo tanto, entendido.
  Otro aspecto de la confidencialidad es la protección del tráfico de los posibles análisis. Esto requiere que para un atacante no pueda ser posible la observación de las direcciones de origen y destino, frecuencia, longitud, puertos y otras características de tráfico, que se podrían utilizar de algún modo.

- Autenticación: La autenticación no es más que la confirmación de que el emisor es quien dice ser. También es la manera de asegurar que el mensaje no ha sido interceptado y reenviado a su destino original. Este proceso se puede llevar a cabo a través del uso de claves, firmas digitales, PINs; según el protocolo de autenticación utilizado.

- Integridad del mensaje: Tal y como ocurría con la confidencialidad, la integridad de mensaje, asegura que la información del o de los mensajes recibidos no han sido duplicados, insertados, modificados, reordenados o repetidos.

- No repudio: Es el proceso por el cual, los usuarios no puedan negar las responsabilidades de las acciones que ellos llevan a cabo. De esta manera se asegura quién ha enviado el mensaje, y también el emisor

- puede certificar si el receptor que ha recibido el mensaje es su receptor original.

- Control de acceso: Es la habilidad de limitar y controlar el acceso a una aplicación o a un dispositivo-ordenador. Para ello, en primer lugar se autentica o identifica al usuario. Si ha tenido éxito, se procede a su autorización para poder utilizar los servicios de la aplicación o del dispositivo.

- Disponibilidad: A disponibilidad se refiere a que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo. Viene provocado a que algunos ataques provocan la reducción (total o parcial) de la disponibilidad de acceso a un dispositivo o una aplicación.

Estos son lo puntos para clasificar la seguridad. A partir de aquí se puede observar que existen distintas maneras de intentar asegurar la información o el acceso legal. De entre ellas, la criptografía (o la transformación de la información), es la técnica de seguridad más antigua de las comunicaciones. Se conoce su uso desde la época de Julio Cesar, y el cifrado que lleva su nombre es la base de los cifrados actuales.

El uso de palabras clave, a través de claves públicas y privadas, es también de uso habitual para poder autenticar y asegurar las comunicaciones.

1.2. Firewalls

La aplicación más utilizada en los últimos años es la archiconocida *firewall (cortafuegos)*. Esta, es una combinación de hardware y software que utilizan las empresas y los usuarios para aislar la red privada del exterior, como si fuera una gran barrera (como se muestra en la **Fig. 1.1**).

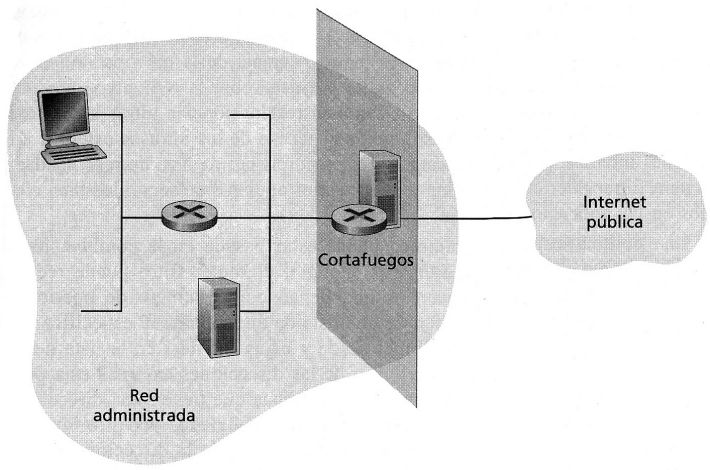


Fig. 1.1 Red administrativa con cortafuegos

Un firewall es un mero control de acceso del tráfico entrante/saliente de la red del usuario. En este control, se revisan los datagramas o paquetes que por él pasan y según las reglas que haya impuesto el administrador de la red, actuará en consecuencia: eliminando, reenviado o preguntando al administrador.

Existen cuatro tipos de firewalls: de filtrado de paquetes, pasarelas de nivel de aplicación, inspección multinivel de estados y *Circuit Level Gateways*. Los dos primeros son los más utilizados, pero es el de inspección multinivel el mejor considerado. La gran diferencia que existe entre ellos, es el nivel de la capa OSI en el que trabajan. El de multinivel, como bien indica, trabaja en diversos niveles (de nivel de red a nivel de aplicación). Todos ellos, estas explicados en el apartado de anexos (Anexo A).

1.3. Amenazas y contramedidas

Todo elemento de red, ordenador o dispositivo con sistema operativo, es susceptible de padecer intrusiones, virus u otros elementos indeseables. En la década de las comunicaciones incluso los móviles comienzan a ser parte de la carnaza para los “phreackers” (“hackers” de los sistemas telefónicos). Este mundo, tiene muchas ramificaciones, pero lo más importante es que cada día tiene más adeptos, y las grandes empresas de seguridad están haciendo el agosto.

En esta sección, únicamente daremos un vistazo a las amenazas más comunes y genéricas en el mundo de las redes, y que por lo tanto, son más probables en ambientes de MPLS y ATM.

1.3.1. Planear

Cualquier atacante que se precie, utiliza la técnica del espionaje para averiguar información sobre su objetivo. A través de las informaciones que recopila al respecto, puede conseguir planear un ataque mejor.

A nivel de red, en algunos tipos de ataques, se deben conocer las direcciones IP de las máquinas y los puertos abiertos, los sistemas operativos que se utilizan y servicios que ofertan. Por lo tanto, podemos llamar planear a la recopilación de información sobre una red o un sistema.

Esta recopilación se puede llevar a cabo a través de intentos de envíos *ping* (si contesta afirmativamente quiere decir que la IP existe). En el caso de querer averiguar los puertos abiertos, se puede hacer un “escaneado de puertos”, Programas como el *Nmap* tienen este objetivo. Su funcionamiento es muy simple, y sólo consiste en ir preguntando secuencialmente a los números de puerto en una máquina y esperar la respuesta. Con esta técnica se puede averiguar tanto los servicios que presta la máquina como las puertas abiertas que deja.

Muchos de los firewalls actuales tienen la capacidad de poder descubrir este tipo de ataques, y acto seguido avisar al administrador de las peticiones que se hacen desde el exterior.

1.3.2. Husmear paquetes

Un husmeador de paquetes es un programa que se ejecuta en un dispositivo asociado a la red. Como se muestra en la figura 1.2, con él los administradores pueden conocer todos los movimientos de la red, con el fin de gestionar y monitorizar la red.
Por otro lado, para los hackers es una gran manera de obtener información. El llamado *eavesdropping* puede facilitar información privada de los usuarios de la red. Con la lectura ilegal de los *payloads*, pueden obtener tanto información de la red como de direcciones de red, el tipo de aplicaciones-servicios que se ejecutan, pero sobretodo indentificadores y contraseñas.

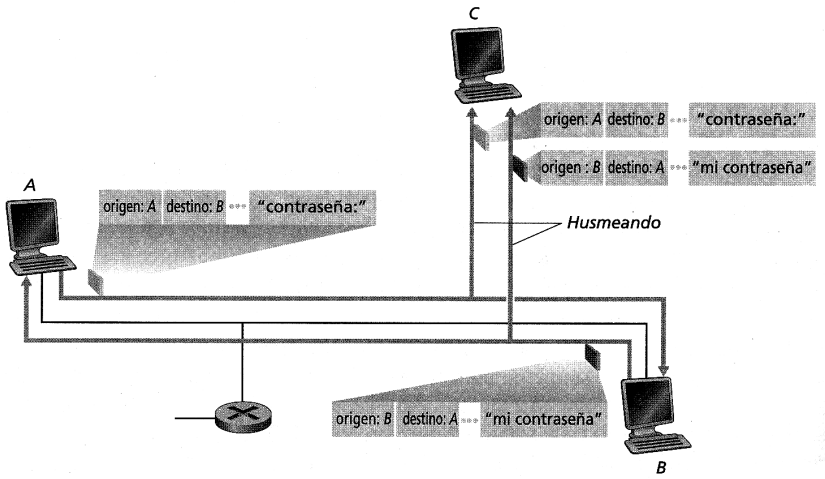


Fig. 1.2 Ejemplo de eavesdropping

1.3.3. Spoofing

Éste, es utilizado en los ataques de denegación de servicio (sección 1.3.4). El spoofing o falsificación es hacer creer al agredido que la web, la IP, el e-mail o cualquier tipo de tráfico de red, es real cuando en realidad una tercera persona es la que lo está generando.

Este tipo de ataques tiene muchas alternativas: podemos encontrar spoofing IP, ARP, Web, DNS e incluso e-mail. Posiblemente el más típico es el que se ilustra en la figura 1.3. Se trata del ataque de spooging IP, y es muy sencillo de ejecutar porque cualquier administrador puede cambiar la IP (192.168.0.5) de su interfaz por otra (172.16.0.6), para, por ejemplo, intentar entrar en una red

restringida a un conjunto de IPs, o como en el caso de la figura, hacer recibir al agredido una información que no había pedido.

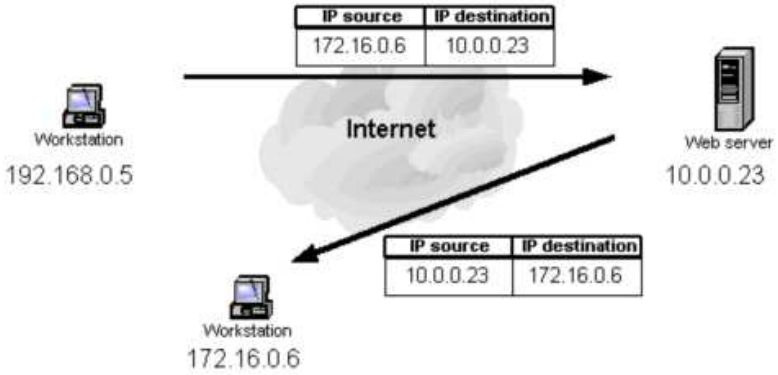


Fig. 1.3 Ejemplo de IP spoofing

Cada vez más, se están buscando maneras para evitar este tipo de ataques y la denegación de servicios que normalmente viene asociada. Estas contramedidas pasan por autenticar que los datos recibidos son verdaderos-originales (como por ejemplo para los e-mails, o para las DNS), como también denegando la entrada a cualquier tipo de tráfico broadcast.

En el RFC 2267 se indica que este tipo de tráfico se puede evitar si los ISPs filtran los ataques desde su origen. Se alega que toda interfaz conectada a un ISP (*Internet Service Provider*) tiene asociada una IP (estática o dinámica) que no puede ser cambiada por el usuario. Por lo tanto, en el momento en que el usuario intente enviar una paquete con otra dirección que no corresponda la suya, se puede filtrar y el ataque quedará neutralizado. Pero la única pega de esta idea es que los ISPs tienen que querer hacerlo.

1.3.4. Denegación de servicio (DoS)

La denegación de servicio o DoS (Denial of Service) tiene por objetivo inutilizar a un elemento de red, un host o una red completa. Este tipo de ataques, consisten en incrementar mucho la carga de trabajo de la infraestructura atacada de modo que no pueda realizar las tareas que tiene encomendadas.

Por ejemplo, en el ataque de inundación SYN, el atacante inunda un servidor con paquetes TCP SYN cada uno con una dirección IP origen falsificada (spoofing). El servidor, al ser incapaz de diferenciar un SYN legítimo de otro falso, reserva el tamaño apropiado para los búferes (de transmisión-recepción) y las variables de conexión, y envía un segmento de concesión de conexión. Pero el atacante por su parte, no contesta a este segmento, dejando al host a la espera con las conexiones abiertas, con lo que el servidor sobrecarga su memoria y finalmente se rinde y cae.

Otro ataque parecido puede ser, enviar fragmentos IP pero nunca los suficientes como para poder completar el datagrama. De tal manera que el servidor va acumulando los fragmentos IP sin poder llegar a procesarlos y llena su memoria.

También existe otro tipo de ataque a terceros, llamado *smurf*. Este ataque consiste en hacer que un gran número de host inocentes respondan a los paquetes ICMP de solicitud de eco (ping), con una dirección IP origen falsa. Esto produce que un gran número de paquetes ICMP de respuesta inundaran al host cuya dirección ha sido robada.

1.3.5. Denegación distribuida de servicio (DDoS)

Éste es un tipo de ataque mucho más potente que el DoS y a su vez más complicado de evitar y de gestar. En este caso el atacante debe instalar y ejecutar un programa esclavo en un conjunto de host sin que los usuarios sean conscientes.
Con un programa maestro, el atacante puede indicar a todos los programas que ha distribuido que ejecuten unos comandos o un ataque preestablecido. La suma de todos los ataques originados desde distintos puntos de la red, siempre tiene resultados devastadores.

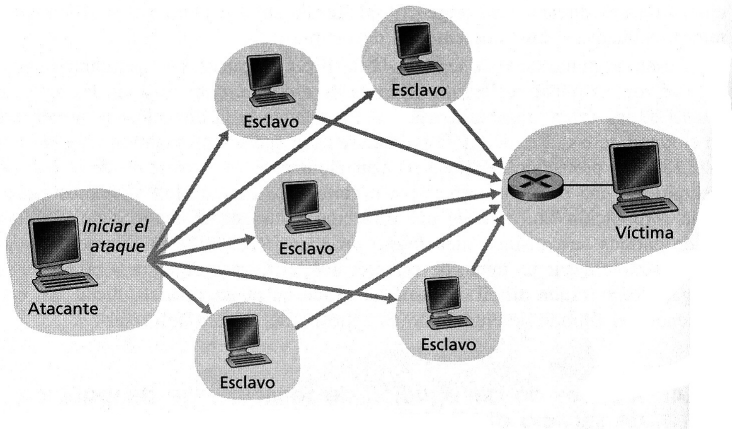


Fig. 1.4 Ejemplo de ataque DDoS

Un ataque como el presentado en la figura 1.4 puede llegar a hacer caer portales de Internet como eBay, Yahoo o el de la CNN, incluso servidores DNS o de correo electrónico.

Las soluciones ante este tipo de ataques (tanto DoS como DDoS) pasa por filtrar todos los paquetes broadcast, tener actualizados los servidores y simples ordenadores de toda la red (Internet), y también seguir las indicaciones del RFC 2267 como ya se ha comentado en la sección *1.3.3*.

1.3.6. Secuestro

Como la misma palabra indica, este tipo de ataques consiste en secuestrar una conexión entre dos puntos finales, de tal manera que el atacante (copiando los datos de ACK, SYN, IP, puertos, etc.) pueda hacerse pasar por uno de los dos puntos finales sin que el otro se de cuenta.

El atacante, en algunas ocasiones, actúa como una pasarela de aplicación, enviando información falsa a los usuarios reales de la conexión sin que ellos puedan notarlo.

1.4. Los peligros de nuestras redes

Después de este pequeño repaso a las distintas amenazas de la red y a algunas de sus contramedidas, sólo cabe listar algunos de los peligros más comunes en infraestructuras ATM, MPLS, y en tecnologías como VPN y BGP.

- En plano de usuario:
  - Observación no autorizada de tráfico de usuarios
  - Modificación de tráfico de usuario
  - Inserción de tráfico no auténtico
  - Suplantación de usuario o conexión
  - DoS del plano de usuario
  - Falsificación de VPNs
- En plano de control:
  - DoS del plano de control
  - Ataques a infraestructuras
  - Desconfiguración de dispositivos
  - Suplantación de servidores para la difusión de información falsa
  - Ataques a protocolos de control (BGP, RIP, etc.)
  - Observación no autorizada de tráfico de control

Para acabar, una frase que resume de la mejor manera este capítulo:

“Lo mejor que podemos hacer es resistir a un cierto conjunto de ataques que conocemos y con los cuales estamos familiarizados. No hay nada en el mundo que pueda protegernos contra nuevos tipos de ataques”

Rolf Oppliger
“*Security Technologies for the World Wide Web”; Artech house*

CAPÍTULO 2. SEGURIDAD EN ATM

ATM surgió como modelo de referencia para integrar todos los servicios en una sola infraestructura. Aportaba una red con QoS, rapidez, eficiencia y seguridad. Fue la primera infraestructura que al ser ideada, se planteo como objetivo la inclusión de un gran nivel de seguridad. Pronto se dieron cuenta de que habían dejando muchas puertas abiertas para los hackers.

Años después, las grandes organizaciones y empresas (Multinacionales, Bancos, Universidades, etc.) se dieron cuenta de que la infraestructura del futuro tenía serias carencias en seguridad. ATM Forum no tardó en reaccionar. La *Security Working Group* de la ATM Forum empezó a trabajar en 1995 para desarrollar una serie de medidas específicas para mejorar la seguridad en ATM. Desde entonces, han desarrollado básicamente dos grandes propuestas: *ATM Security Specification Version 1.0* (Febrero 1999) y *ATM Security Specification Version 1.1* (Marzo 2001).

Durante este capítulo trataré de explicar las carencias de la primera versión de ATM, para después ver como el ATM Forum incorporó una serie de servicios de seguridad para solventar la mayoría de los problemas. De esta manera sólo restará dar unas pequeñas conclusiones de la seguridad que ofrece ATM.

2.1. El modelo ATM

ATM Forum no podía romper su modelo original para realizar otro, sino que debía trabajar sobre la base que ya tenía. Así pues, ATM Forum trabajó basándose en el modelo de referencia que se muestra en la figura 2.1.

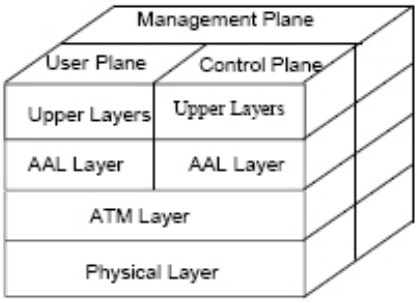


Fig. 2.1 Modelo de referencia ATM

Básicamente podemos observar que el modelo trabaja con tres planos:

- Plano de usuario: Este es el plano que soporta la transferencia de datos entre puntos finales ATM a lo largo de un circuito virtual permanente (*Permanent Virtual Circuit* - PVC) o un circuito virtual conmutado (*Switched Virtual Circuit* - SVC). Este tráfico puede ser originado por un protocolo de capas altas (como IP), o puede ser directamente de una

aplicación de ATM (conexiones LANE, direcciones ATM de IP/ATM, etc.).

- Plano de control: Se responsabiliza del establecimiento de las SVC. Los protocolos de señalización que ejecutan los establecimientos de conexiones dinámicas son parte de este plano. También contiene el tráfico de protocolos de enrutado que distribuyen la topología de red y la información de estado a todos los switchs ATM.

- Plano de gestión: Este tiene la responsabilidad de: permitir a los dispositivos de igual nivel a pasarse información específica de gestión, y permitir configuración remota y monitorización de estados de los elementos de la red ATM.

Como se puede observar, cada plano contiene cuatro niveles: nivel físico, nivel ATM, nivel de adaptación ATM (*ATM Adaptation Layer* - AAL) y capa alta de protocolos o aplicaciones.

- Nivel físico: Es el nivel que proporciona las conexiones entre elementos de la red ATM.

- Nivel ATM: Este nivel se responsabiliza de conectar las celdas a las conexiones VC. Para el plano de gestión ATM especifica el uso de celdas OAM (*Operation, Administration and Mantinence*) que permiten a los dispositivos crear una comunicación para gestión dentro del VC del plano de usuario.

- AAL: Con este se proporciona una interfaz que adapta las celdas de ATM a los frames de las aplicaciones o protocolos, y viceversa.

- Capa alta de protocolos y aplicaciones: Usa los servios proporcionados por el AAL. Para el plano de usuario están incluidos protocolos como IP junto con las aplicaciones de ATM que acceden al AAL directamente a través de APIs (aplicaciones de interfaz de programadores). Para el plano de control, este nivel incluye el protocolo Q.2931 y el PNNI 1.0. Para el plano de gestión, incluye los protocolos de gestión de elementos de red y el ILMI (*Integrated Local Management Interface*) que permite la autoconfiguración de elementos.

La ATM Forum, cogió todo este entramado de planos y niveles, e incluyó una serie de mejoras a estos elementos. La verdad es que todo el trabajo se volcó en los planos de usuario y de control; el de gestión lo dejaron de lado como un punto a trabajar en el futuro. Aunque algunas de las mejoras incluidas en el plano de usuario también se reflejan en el plano de gestión.

2.2. Las grandes amenazas de ATM

Como todas las redes, ATM tiene una serie de puntos débiles característicos de su infraestructura y sus protocolos. La amenaza más notable entre todas es la de spoofing. Esta amenaza tiene muchos años de antigüedad y aunque durante las próximas páginas se den algunas contramedidas, aún hoy es caso de estudio.

Así pues, estas son, a grades rasgos, las amenazas de "la versión pura" de ATM:

- Eavesdropping (fisgoneo), violando la privacidad de las comunicaciones
- Modificación desautorizada de la información
- Falsificación de la identidad (tanto de remitente como de receptor)
- Denegación de servicios, bloqueando el acceso a la conexión de los usuarios ,o por la inundación o descarte de mensajes, que provoque la saturación de los dispositivos
- Robo de la VC (*Virtual Connection*) de otro usuario

Por lo que podemos observar, las grandes amenazas pasan por el *spoofing*, el *eavesdropping* y el *DoS*, como más importantes.
Dónde más vulnerables se encontraban en ATM era en las fases de inicialización de las conexiones y en el traspaso de las contraseñas. Por ello se intentó incrementar la autenticación en los servicios y en los establecimientos de conexiones o en el ingreso de un nuevo miembro (router, punto final, etc.)

2.3. Objetivos de ATM Forum

ATM ya incorporaba algunas barreras de seguridad. No se implantó desnudo ante las adversidades pero incluso así dejó muchos puntos flacos.
Las primeras versiones, ya incorporaban filtrado de direcciones tanto para el ingreso de clientes (en el NSAP) como para la incorporación de nuevos miembros ATM. Los dispositivos ATM eran agrupados en bloques lógicamente separados. Esto significa que sólo leían el tráfico de su grupo. El único problema residía en aquellos switchs que formaban parte de diversos grupos a la vez (como switchs puente). Pero se solucionaba con el filtraje de direcciones o con el control de listas (para agrupaciones LANE).
A todo esto habría que añadir la posibilidad de encriptar el tráfico (por ejemplo HTPP) o autenticar. Aún así, no se aseguraban todos los tráficos de la red (usario, control, gestión).

En el capítulo anterior se dijo, que antes de empezar a incluir parches en nuestros sistemas, lo principal era descubrir los puntos donde se es vulnerable. Después de observar detenidamente aquellos puntos donde la integridad de sus sistemas corría peligro, se impusieron una serie de objetivos de seguridad que debían conseguir:

- Autenticación
- Integridad de los datos
- Responsabilidad
- Disponibilidad de los servicios

Estos no distan de los objetivos de seguridad que deberían tener en cualquier red. Entre ellos, la integridad de datos es un objetivo claramente destinado a evitar los robos o fisgoneos de datos. De esta manera se quiere impedir que los atacantes puedan recopilar información (trascendente o no) que pueda provocar el robo de servicios o de bienes económicos (robo en cuentas de bancos, compras con los datos de otras personas, etc.).

La autenticación por su parte, se destina a conservar la identidad de cualquiera de las operaciones que se realizan en la red. Desde los propios usuarios a todas las comunicaciones de control y mantenimiento que se efectúan entre los dispositivos de red. Por otro lado, la responsabilidad tiene como objetivo la imposibilidad de poder hacer un movimiento sin que se pueda evitar certificar la identidad del responsable. Por último, con la disponibilidad de los servicios se quiere evitar que los usuarios no puedan utilizar los servicios que han contratado. Es el objetivo directamente vinculado a los ataques DoS, que perjudica a los niveles de QoS.

De acuerdo con estos objetivos, se marcaron las principales funciones a crear. Estas son:

- Verificación de identidades
- Acceso y autorizaciones controladas
- Protección de la confidencialidad
- Protección de la integridad de los datos
- No negación de responsabilidades
- Registro de las actividades de la red: capacidad de la red para registrar los movimientos de la red, con la intención de mantener el sistema seguro
- Aviso de alarmas de seguridad
- Capacidad de la red para auditar: al generarse una alarma de seguridad, la red debe poder consultar los registros e identificar la infracción y el infractor
- Gestión de la seguridad
- Recuperación de la seguridad: capacidad de la red para recuperarse después de cambios (permitidos o no) en el estado de la seguridad

2.4. ATM Security Specifications 1.x

Antes de que el grupo de trabajo de la ATM Forum se pusiera manos a la obra, las PVCs y los filtros de las NSAP eran las grandes bazas para asegurar la red. El gran problema que encontraron fue que los atacantes optaban entonces por amenazar otros puntos de la red. Por ejemplo, las PVCs protegían la

información en los VC (Circuitos Virtuales), pero dejaban al descubierto la confidencialidad del tráfico que atravesaba redes públicas.
Otro de los grandes problemas fue que, la posibilidad de encriptar mediante claves privadas debía hacerse a velocidades muy altas ya que las redes a principio de este siglo alcanzaban el Gigabit de velocidad.

Actualmente existe únicamente una versión del llamado *ATM Security Specifications*, al que llamaron "versión 1.0" (Febrero 1999). Además, en marzo del 2001 sacaron a relucir las actualizaciones de las diferentes medidas que habían adoptado en la versión 1.0 (ha esta se la llamó "versión 1.1"). Aunque los elementos centrales no han cambiando, se cambiaron, eliminaron, añadieron y sobretodo clarificaron, algunos procesos y algoritmos utilizados en la primera versión.

Durante esta sección del capítulo, se comentaran aquellos puntos importantes de esta especificación de seguridad. Sobretodo dando importancia a aquellos procesos y elementos mejor considerados por el grupo de trabajo.

2.4.1. Aspectos importantes

El gran objetivo de esta especificación era proteger el tráfico del plano de usuario. Como se puede observar en la figura presentada (**Fig. 2.2**) en el documento de esta especificación, la gran olvidada es el plano de gestión. Aún así, algunos de los servicios de seguridad destinados al plano de usuario, también ayudan a proteger este plano.

	User Plane	Control Plane	Management Plane
Authentication	X	X	
Confidentiality	X		
Data Integrity	X	X	
Access Control	X		

Fig. 2.2 Servicios tratados

Los elementos clave del modelo de seguridad de ATM son los son los SAs (*Security Agents*). Cada SA, es el responsable de desarrollar las asociaciones de seguridad entre los distintos elementos de la red (incluidos los puntos finales). Estas asociaciones pueden ser configuradas tanto manualmente como a través de los SMEs (*Security Message Exchange*). Este, es un protocolo que crea estas asociaciones automáticamente a través de las SVCs. Todo esto ayuda a establecer los servicios de seguridad creados para este modelo.

Así pues, SAs, SMEs y Servicios serán los "elementos" que veremos a continuación en este resumen de la especificación (v1.x).

2.4.2. Security Agent

El SA es el responsable negociar y proporcionar los servicios de seguridad disponibles. Cuando dos o más SAs se asocian, a esta unión se le denomina asociación de seguridad. Estas asociaciones son creadas para cada servicio de seguridad que se establece a cada VC del plano de control o de usuario. En ella, se determinan las particularidades de los servicios, incluyendo algoritmos, los parámetros del algoritmo escogido, las claves de seguridad, y las etiquetas de sensibilidad (que indican el nivel de protección que necesitan los datos).

Estos elementos situados en los extremos de la red, proporcionan seguridad *end-to-end*. Los SAs localizados en los switches proporcionan un gran volumen de servicios de seguridad a los puntos extremos, pero la asociación de seguridad sólo abarca parte de los VC creados entre ellos.

En el caso en que fuera necesario que en una misma conexión VC, se necesitaran distintos servicios, se utilizaría otro par de SAs. Para que no hubiera problema de solapamiento de los servicios, en la especificación se establece la necesidad establecer una topología de niveles. Además de limitar el número de niveles a 16 en los casos de integridad y encriptación, o a 256 para los servicios proporcionados por el protocolo SME (por ejemplo autenticación).

La seguridad se proporciona en distintas fases durante la asociación de seguridad: durante el establecimiento de una asociación de seguridad y durante el tiempo de vida del circuito virtual.

Los servicios que son proporcionados durante el establecimiento de la seguridad, se establecen gracias al protocolo SME. En un servicio basado en SME, cada uno de los miembros de la asociación es “etiquetado”. Uno de ellos es llamado “iniciador” (*initiator*); el cual es el responsable de iniciar el intercambio del protocolo SME. El otro es proclamado como “contestador” (*responder*), que es aquel que espera al primer mensaje SME del iniciador. Estos roles se pueden determinar de forma automática a través de la señalización SVC o a través de la gestión de las PVCs.

Como se puede ver en la figura 2.3, un SA está compuesto por 4 elementos con los que se consigue asociar y gestionar los servicios de los dos SAs asociados.

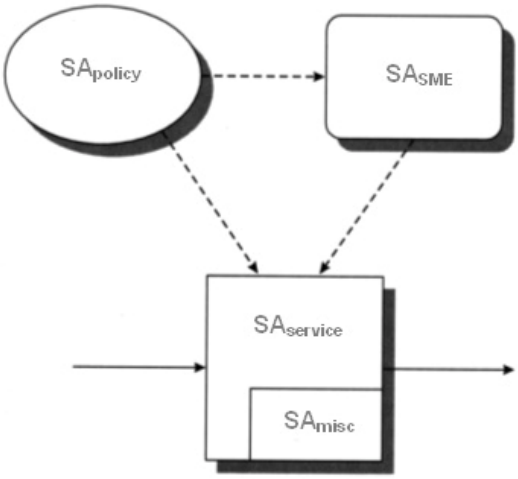


Fig. 2.3 Relación entre los elementos de una SA

Estos cuatro elementos tienen las siguientes funciones:

- $SA_{service}$: Este elemento implementa el servicio de seguridad que se aplica al VC durante su tiempo de vida. Este elemento es configurado por el SA_{policy} y el SA_{SME}, y trabaja junto con el SA_{misc}; como se muestra en la figura 2.3
- SA_{misc}: Es este caso, este elemento ejecuta diversas funciones, como encargarse del mantenimiento de la asociación durante la transferencia de datos. Los servicios que proporciona este elemento son: clave de sesión y sincronización criptográfica.
- SA_{policy}: Este determina y define los servicios de seguridad, algoritmos y parámetros del algoritmo que el SA implementa en el VC durante el establecimiento de la asociación y el tiempo de vida del VC.
- SA_{policy}: Este en cambio se ocupa de implementar los servicios durante el establecimiento de la asociación (autenticación, intercambio de clave, intercambio de certificado, negociación, control de acceso, etc.). Es configurado con las políticas de seguridad pertinentes por el SA_{policy}.

2.4.3. Métodos de transporte de mensajes de seguridad

Existen tres métodos para el transporte de los mensajes de seguridad que deben intercambiar los agentes para establecer la asociación entre ellos.

2.4.3.1. Signaling-Based

Este método utiliza los mensajes de señalización para transportar la información de seguridad.

A modo de ejemplo, en la figura 2.4 se muestra un sistema final (izquierda) perteneciente a un red privada. Este elemento decide solicitar una conexión (SVC_{setup}) a otro sistema final de la misma red pública.
Cada uno de ellos cuelga de la red pública "junto con" un SA, los cuales les proporcionaran servicios de seguridad.

Como se puede observar, el SA más cercano a la red privada se establece como "iniciador" (ya que el mensaje de conexión lo recibe de una red privada). Este SA, añade al mensaje de petición de conexión elementos de información (*Information Elements* - IE) con información relacionada con la seguridad para el SA remoto (a estos IE de seguridad se les llama SIE). Este mensaje atraviesa la red pública, que lo procesa y lo envía hacia el SA del otro extremo.

En el otro extremo, el SA recibe el mensaje y se identifica como el "contestador". Acto seguido inspecciona los elementos IE que incluye, y si todo es correcto, lo procesa y envía el mensaje a su destinatario. Si este desea aceptar la conexión, responde a la petición con un mensaje $SVC_{connect}$. En el camino de un SA a otro, se enviará más información a través del IE. Si el SA iniciador acepta, envía un mensaje de $SVC_{connect}$ a su destinatario, y se acaba de establecer la conexión.

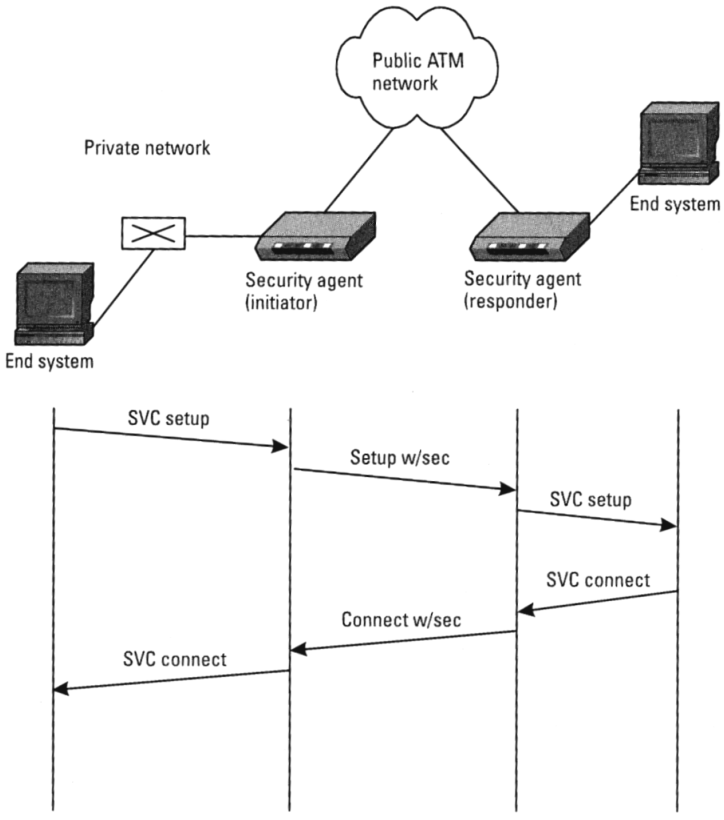


Fig. 2.4 Ejemplo de Signaling-based

2.4.3.2. In-band

El método In-band utiliza el VC del plano de usuario, por eso los mensajes no aumentan de tamaño por la información adicional para las SA.

Esto se puede observar claramente en la figura (**Fig. 2.4**) que representa los mismos elementos que en el caso anterior. Aunque aquí se utilizan PVCs (*Permanent Virtual Connections*) para el envío de los mensajes. Un tipo de conexión que no soporta en anterior método.

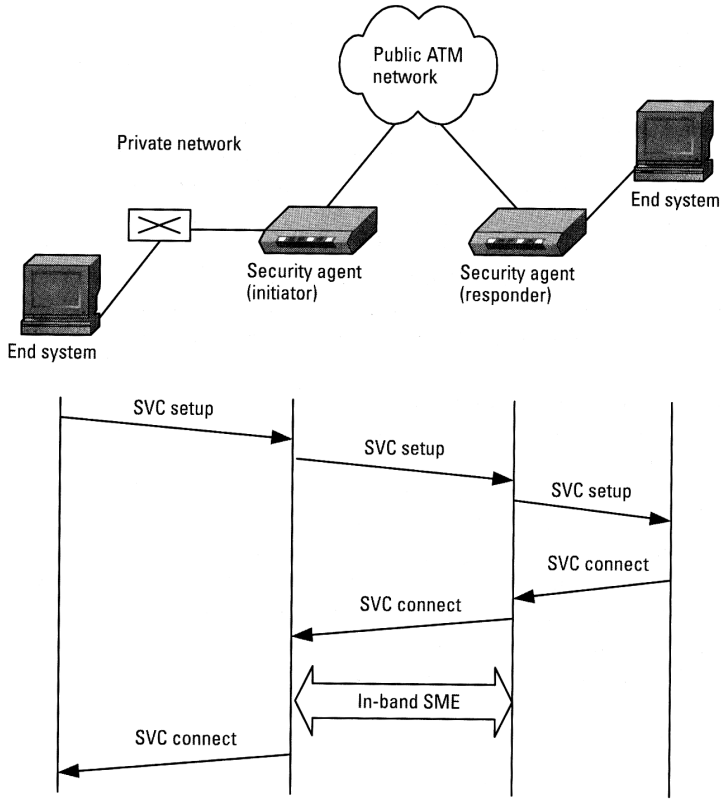


Fig. 2.5 Ejemplo de In-band

Como se puede ver, ni el mensaje de inicialización de conexión ni el de conexión, enviados de SA a SA no llevan ningún tipo de información añadida. Por ello, para que los SAs puedan intercambiar la información referente a la seguridad de la asociación, se bloquea el tráfico. Para poder comenzar el intercambio, se determinan los roles de cada SA. Una vez establecidos, y como en el método anterior, el "iniciador" empieza el protocolo. Una vez el protocolo se ha completado, los dos SA desbloquean el tráfico y se puede establecer la conexión entre los dos sistemas finales.

La gran desventaja de este sistema es que utiliza el protocolo "three-way" y requiere más tiempo para poder establecer la asociación. En cambio, el método signaling-based, utiliza el protocolo "two-way", que a parte de necesitar 2 envíos, puede utilizar el la señalización del VC para intercambiar la información.

Por el contrario, signaled-based no puede ser utilizado en redes que no soportan SSIE (un estándar para las cabeceras de SME que se utiliza para el envío de la información de intercambio entro los distintos SAs). Aunque es difícil encontrarse en esta situación, es un handicap a tener en cuenta.

2.4.3.3. Signaling-based con In-band Fallback

En caso en que no se conozca si la red puede o no soportar SSIE, se escoge por defecto la opción de utilizar el método in-band. Otra posibilidad, es empezar utilizando signaled-based y si falla la comunicación, reemplazar el método por In-band.

De todas maneras, se puede utilizar ambos para sacar lo mejor de cada uno. Por ejemplo (si la red soporta SSIE), utilizando signaling-based para la autenticación y la negociación de los algoritmos de encriptación durante la fase de in-band.

2.4.4. Los servicios de seguridad para el plano de usuario

Estos servicios se extienden en dos categorías: durante el establecimiento de la asociación de seguridad y mientras la VC siga creada.
Los servicios de seguridad iniciales son proporcionados por el protocolo SME, a través de uno de los mecanismos tratados en la sección anterior. Con ello se pueden proporcionar los siguientes servicios para el plano de usuario:

2.4.4.1. Autenticación inicial

Para este servicio, existen dos posibilidades para el envío de parámetros: a través de *signaling-based* o *in-band* a través del canal de datos.

- Signaling-based: Este consiste en incorporar-añadir un elemento de información de seguridad (SIE – Segurity IE) al inicio, y mensajes de conexión. Este intercambio de SIE permite a los elementos de la conexión negociar los servicios de seguridad y los mecanismos, e intercambiar las claves de encriptación utilizadas para proteger los datos. Todo ello juntamente con el resto de los datos intercambiados por los elementos de la red.
  Para este caso, existen tres niveles de claves: la clave de sesión, utilizada para encriptar datos; la clave *master*, utilizada para encriptar claves de sesión para cuando se actualizan las claves durante la conexión; y la clave *top-level*, que es una clave asimétrica utilizada para autenticar y inicializar la primera clave de sesión, y la clave *master*.

- In-band: En vez de enviar los datos de seguridad junto con el resto de datos de conexión, se puede parar el tráfico de datos cuando el elemento que hace esclavo de la conexión envíe la aceptación de la conexión. La negociación de seguridad por lo tanto, se realiza a través del canal de datos, y al finalizar, se desbloquea la transferencia de datos.
  Para que el receptor sepa que la negociación se establecerá in-band, se indica esta elección a través de un SIE en el mensaje de inicio.
  En lo que respecta a la negociación, se encapsula en los mismos SIEs que en el caso anterior.
  Una ventaja de esta solución respecto la otra, es que la longitud de la SIE no está limitada, por lo que pueden ir incluidos los certificados de las claves, por ejemplo.

2.4.4.2. Control de acceso

En este caso, se asocia a cada VC una etiqueta de restricción de libertad o sensibilidad de datos. Con lo que se incluyen un conjunto de reglas para aquellos usuarios con preferencias de servicios y sobretodo para que se otorguen los servicios contratados (ni más ni menos).

También se incluyen servicios de seguridad para el plano de usuario para proteger el intercambio de datos mientras la conexión virtual permanece activa.

2.4.4.3. Autenticación del origen de los datos/Integridad

Este permite asegurar que los datos recibidos por un SA no han sido modificados (por posibles alteraciones o reordenaciones) en su trayecto. Para proporcionar este servicio, los frames AAL son protegidos añadiendo un *checksum* criptográfico. Todo este proceso se lleva a cabo añadiendo una firma digital dentro del SDU (*Service Data Units*) o mensaje de usuario. Existen protocolos de capas altas que pueden detectar la reordenación (como TCP), y este servicio puede ser desactivado. Pero sin embargo existen otras aplicaciones en que añadir una secuencia de números en la AAL SDU ayuda a proteger los datos.
Los algoritmos que en este caso ayudan a generan el checksum o códigos de *hash* pueden ser: DES, FEAL y Keyed MD5.

2.4.4.4. Confidencialidad

Con este servicio se protegen los datos para asegurar la confidencialidad; estos son encriptados celda a celda. Únicamente se encriptan los 48 bytes de *payload*. La cabecera por lo tanto no queda encriptada. Para la encriptación se incluyeron diferentes algoritmos: DES (Data *Encryption Standard*), TripleDES,

Diffie-Helman, RSA y FEAL. También se especifican las diferentes maneras de como se deben encriptar y desencriptar los datos por los algoritmos anteriores, o lo que es lo mismo, se especificaron los modos criptográficos de operación: ECB (*Electronic CodeBook*), CBC (*Cipher Block Chaining*) y el Counter mode.

2.4.5. Los servicios de seguridad para el plano de control

La ATM Forum descubrió que el plano de control podía ser atacado por usuarios externos a través de la introducción de mensajes falsos. Por ello optaron por proporcionar autenticación de origen de datos/integridad utilizando claves preestablecidas. De esta manera podían descubrir el origen de los mensajes y evitar la repetición o reordenación de estos.

Sin embargo, también sería necesario encriptar los mensajes del plano de control, como se hace en el plano de usuario, para poder evitar que ningún atacante pudiera modificar mensajes de señalización (como por ejemplo el "connect" y el "setup" para establecer la asociación de seguridad). Aunque en la versión 1.1 no se proporciona ningún tipo de mecanismo para ello.

2.4.6. Los servicios de soporte

A parte de los servicios a cada plano (definidos en los dos puntos anteriores), también se proponen servicios para garantizar la escalabilidad y el alto rendimiento de los servicios de seguridad.

2.4.6.1. Declaración y negociación de seguridad

Con este servicio se establecen los servicios comunes y los parámetros para la asociación de seguridad a través del protocolo SME. Estos parámetros son los servicios de seguridad, los algoritmos y los parámetros del algoritmo escogido. De todas formas, estos parámetros pueden ser estipulados manualmente, pero podría ser una tarea imposible para grandes redes.

La *declaración* permite al "iniciador" definir que servicios, algoritmos y parámetros quiere utilizar en la asociación de seguridad. El "contestador", como vimos en la sección 2.4.3, revisa la declaración y acepta o deniega la demanda.

En la *negociación* en cambio, el "iniciador" envía una lista de las opciones que podría soportar en la asociación, y el "contestador" elige la que más le guste. Esta opción requiere que se utilice el protocolo SME three-way. En cambio para la declaración se utiliza el protocolo SME two-way.

2.4.6.2. Actualización de claves de sesión

Para que las conexiones encriptadas sean tan seguras como sea posible, ATM Forum determinó que debían actualizarse las claves cada cierto tiempo. Como las células OAM proporcionan un servicio sincronizado con los datos, se escogieron sus celdas como portadoras de las nuevas claves.
Para esta transmisión se definen dos pasos:

- *Primero:* Se envía una clave de sesión cifrada con la clave master gracias a una celda OAM llamada celda SKE (Sesion Key Exchange).

- *Segundo:* Las claves de sesión se activarán gracias a una celda llamadas SKC (Session Key Changeover). Durante la transmisión de estas celdas, el tráfico de datos se bloqueará para que los primeros datos recibidos después de la primera celda SKC OAM, sean descifrados con la nueva clave.

Con todo este trajín de celdas, si una de las dos celdas (SKE y SKC) se pierde durante la conexión, la información no podrá ser desencriptada correctamente. Por ello ATM Forum propuso enviar un flujo de SKEs iguales, seguido de un flujo de SKCs también iguales.

2.4.6.3. Intercambio de claves

Permite que dos SAs compartan las claves para la poder ejecutar los servicios de encriptación o la integridad de datos. Este intercambio de claves, como ocurre con la autenticación, puede ejecutarse con el algoritmo simétrico (clave secreta) o asimétrico (clave pública). Además, este intercambio puede ser bidireccional o unidireccional.

2.4.6.4. Intercambio de certificado

Este servicio permite a dos SAs enviar los certificados de sus claves públicas al otro, como ayuda para las funciones de intercambio de claves y autenticación inicial.

Estos certificados, son creados para aquellos casos en que los atacantes disponen de pares de claves publicas/privadas. Con estos certificados, se puede demostrar que las claves intercambiadas no son falsas.

2.4.7. Security Message Exchange (SME)

El protocolo SME es un mecanismo fundamental para la seguridad, ya que es el responsable del establecimiento de las asociaciones de seguridad. El procedimiento para establecer una asociación de seguridad contiene dos procesos: la identificación del SA, que debe responder al deseo de asociación, y la declaración o negociación del deseo de servicios de seguridad, algoritmos y parámetros para o con el otro SA.

Como ya se mostró durante el 2.4.4, se especifican dos variantes del protocolo SME: el *two-way* y el *three-way*. El primero de ellos se utiliza dentro de la señalización SVC con la utilización de dos flujos de mensajes punto a punto. En cambio, el three-way se utiliza en el VC del plano de usuario después de la transferencia de datos.

2.4.7.1. Direccionamiento del SA

Para poder establecer una comunicación, los elementos siempre deben indicar la dirección donde se encuentra su interlocutor. Para ello, por lo tanto, debe existir un direccionamiento.
En el caso de los SA, existen dos mecanismos de direccionamiento:

- Direccionamiento explicito: Usa un identificador único que debe ser conocido a priori por el SA que inicia el intercambio. Para este mecanismo existen dos formatos: AESA (ATM End System Address) o dirección NSAP, y el X.509 Distinguished Name o SA ID.

- Direccionamiento implícito: Este mecanismo permite que el “iniciador” especifique con que “contestador” quiere establecer el acuerdo, indicando la red a la cual quiere alcanzar. Esta opción se utiliza cuando el “iniciador” no conoce la dirección del “contestador”.

El problema del primero es que el “iniciador” debe conocer la dirección para poder establecer la comunicación. Por otro lado, en el segundo el problema reside cuando más de un SA puede hacer de intermediario del “contestador”, y se debe determinar uno.

2.5. Apuntes finales

Aunque el resumen de los servicios de seguridad presentados ya da una idea general, existen más propuestas, no directamente expuestas con este paquete de seguridad, pero comentadas entre los miembros del ATM Forum.

Entre finales del siglo pasado y principios de este, básicamente existían dos puntos discutidos por aquellos que intentaban mejorar ATM. El primer punto

tiene como principal reclamo, los firewalls. Existen dos ideas fundamentales al respecto: colocar un firewall en mitad de la VC entre dos puntos finales, o situar dos firewalls, uno por cada usuario. El primero indica que esta solución aportaría más seguridad para los intercambios de claves, y para el resto de gestiones. El segundo, únicamente lo coloca para otorgar más seguridad al intercambio de las claves, que consideraba que tenía un alto riesgo de ser atacado.
Sean o no buenas ideas, la colocación de firewalls empezaba a ser parte de las discusiones en seguridad (aunque la ATM Forum incluyó filtros de direcciones en la especificación de seguridad). Hoy en día este es un elemento muy utilizado, casi imprescindible, como pudimos ver en el capítulo anterior.

El otro punto importante que emergía era la incorporación de VPN a las redes ATM. *David Ginsburg*, incluso defendía la idea de utilizar etiquetas para mejorar la seguridad del tráfico, y prescindir de los PVCs como hasta entonces. Incluso, para aquellos usuarios que necesitasen más seguridad defendía la posibilidad de utilizar IPsec para mejorar las prestaciones de encriptación y autenticación de usuario.

Existen también otras propuestas para mejorar el nivel de seguridad de ATM de aquellos años (1999 – 2000). Como ejemplo la propuesta de la utilización del paquete SCAN (Secure Communications in ATM Networks), que rizaba el rizo en cuanto a autenticación e encriptación se refiere. Una propuesta cercana a la que hizo ATM Forum, pero intentado mejorar aspectos como la actualización de claves de servicio, o la conexión de VCs.

Con estas propuestas o sin ellas, el Grupo de trabajo de ATM Forum había creado una especificación que protegía las redes ATM de los ataques más comunes. La amenaza de la que más se protegía era del spoofing (y por lo tanto también un poco de DoS) otorgando a la red mayor autenticación e integridad de los datos. También se evita el *eavesdropping* o el robo de servicios con la utilización de algoritmos cifrado.

En resumen, consiguieron ofrecer una infraestructura segura (no se puede saber hasta que punto) pero que costaba mucho de renovar. Cualquier actualización de los servicios provoca un grabe problema de gestión, y es una de las grandes trabas para mantener actualizadas las redes en contra de las amenazas. Posiblemente ATM era totalmente segura hacia el año 2001, pero es seguro que hoy no es segura del todo. Y es posible porque sean detectado robos de datos de tarjetas de crédito en algunos bancos norteamericanos que utilizaban redes ATM (“Your ATM is not very safe”; Brian Bergstein).

De todas formas, la ATM Forum no ha hecho ninguna revisión-actualización de seguridad desde el año 2002. Talvez hayan tirado la toalla en su lucha con MPLS, aunque mucha gente intente buscar “peros” a MPLS, comparándolo con ATM. Sea o no por ello, últimamente se dedican a buscar soluciones para unir MPLS con Frame Relay o ATM.

CAPÍTULO 3. SEGURIDAD EN MPLS

Llegado este punto del trabajo, todos vemos claro que MPLS surgió como gran alternativa de futuro para hacer de las *backbones* redes más flexibles y eficaces. Ante él, existía (y aún existe) un arduo camino hasta que sea considerado por TODOS como un tecnología solvente y adecuada.

ATM dejó el listón muy alto. Todos los que habían trabajado con esta tecnología eran reacios a tener que cambiar a una tecnología que trabajaba con IP. Y la idea de que en el corazón de la red se trabajara a nivel 3 no les gustaba ya que entendían que así el corazón de la red (core) dejaba de ser seguro. En todo esto existe parte de verdad, pero como veremos a continuación, el core, aún trabajando con IP, es igual de inseguro que ATM.

Para abordar esta parte del trabajo, continuaremos "atacando" la seguridad de las redes con la misma estructura que en el caso anterior (*Capítulo 2: "Seguridad en ATM"*). De esta manera podremos observar mejor las virtudes y las debilidades de cada una.

Por ello, durante la primera parte de este capítulo se mostrará el modelo con el que trabaja MPLS, pero esta vez guiando más la vista hacia el aspecto de la seguridad. Con ello, pasaremos a conocer las grandes amenazas de MPLS para posteriormente, explicar si son una amenaza real, y si realmente lo son, como se puede proteger la red.

3.1. El modelo de seguridad de MPLS

Cualquier institución, proveedor de servicios o empresa que contenga una red de ordenadores u otros dispositivos, debe procurar aplicar a la red una buena protección contra las amenazas. Para ello debe instalar antivirus, firewalls y cualquier otro tipo de software o hardware acorde con sus necesidades: todo depende de si tiene una intranet, una extranet, o por ejemplo acceso a Internet.

De todos modos, los proveedores de servicios tienen la desgracia de tener que pensar en todo ello, y adaptarlo para que miles de dispositivos conectados a sus redes puedan disfrutar de una buena protección.

Tanto MPLS como cualquier otra tecnología debe (o debería) asegurar que sus redes pueden ofrecer una serie de servicios básicos como confidencialidad, disponibilidad, integridad y un rápido restablecimiento de las conexiones en caso de fallo. Para aplicar todo esto, es necesario crear una buena política de seguridad y plasmarla en un modelo acorde con los servicios que le gustaría ofrecer.

El modelo utilizado para MPLS VPN surge de las especificaciones formuladas en el RFC 4111 ("*Security for Provider Provisions VPNs* – PPVPN"). En él se

tratan las características fundamentales que deben seguir las redes de servicios para poder afrontar con solvencia los peligros de las redes compartidas.

3.1.1. Modelo de seguridad básico

En la figura se puede observar el modelo de seguridad básico utilizado en las redes MPLS VPN. Se pueden denotar la existencia de tres "módulos" diferenciados: las VPNs de los usuarios, las VPN de la red MPLS VPN y el core de la red MPLS VPN (como se ilustra en la figura 3.1).

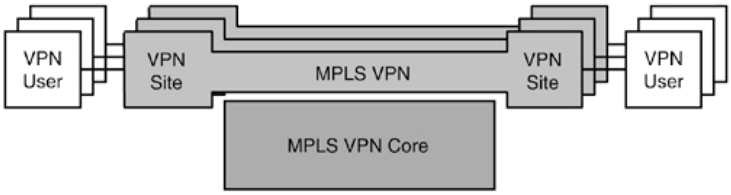


Fig. 3.1 Modelo de referencia de seguridad base

Si concretizamos un poco más, se puede observar que no existe ninguna conexión con ninguna red externa (Internet o extranet). Las únicas conexiones que existen, son las que unen las VPN de los usuarios con su respectiva VPN. No existe por lo tanto ninguna conectividad entre VPNs distintas. El otro punto a tener en cuenta, es la inexistencia de vínculo entre el core y las VPN existentes.

Por lo tanto, en este modelo básico se puede observar que existe una gran independencia de las VPNs con respecto al resto de VPNs y la red core.

3.1.2. Modelo de seguridad con extranet o Internet

Como caso práctico, el modelo básico resulta muy poco atractivo ya que no ofrecer ningún tipo de servicio alternativo. Algo que aporte más versatilidad a las "simples" conexiones entre sedes de la misma empresa.

Pongamos por caso que una empresa de apartamentos con diferentes sedes repartidas por distintas ciudades, contrata un servicio de domótica a una empresa especializada. Talvez, les saldría a cuenta conectar sus redes para poder crear un servicio más personalizado, y donde se pudieran controlar mejor las instalaciones. A esta interconexión se le llamaría extranet, y es lo que se representa en la siguiente figura (**Fig. 3.2**).

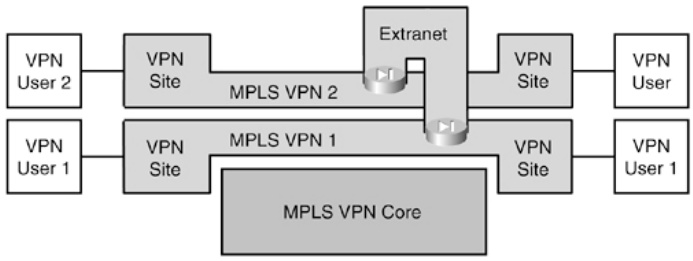


Fig. 3.2 Modelo con extranet

Esta vinculación, desde el punto de vista de MPLS, supone la unión de dos (o más) VPNs para formar sólo una. En cualquier caso, el resto de conexiónes permanecen igual (el core no tiene ninguna vinculación con las VPNs). Como detalle, denotar que en las conexiones de cada empresa (*user 1* y *user 2*) con la extranet, se sitúa un firewall/NAT para asegurar la privacidad y evitar solapamientos de direcciones entre redes.

Otro caso muy común, es la vinculación de una empresa a Internet. En la figura 3.3 se muestra este tipo de conexión que, como en los casos anteriores, no representa ningún tipo de amenaza para la seguridad del core, al menos en su modelo más simple.

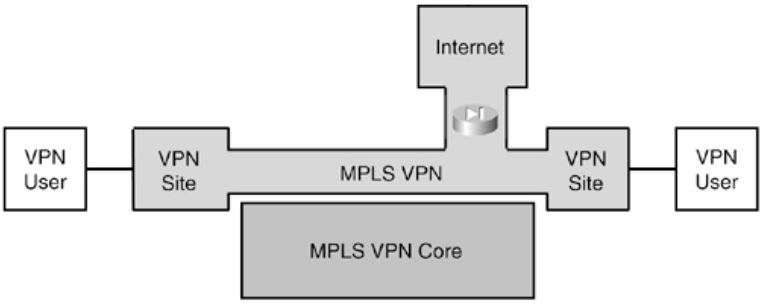


Fig. 3.3 Modelo con Internet

3.1.3. Modelo de seguridad con diversos proveedores MPLS

Hasta el momento se han tratado los casos en que las diferentes VPNs viajaban a través de una única red backbone. Pero, como ya se ha dicho antes, en el mundo real existen otro tipo de necesidades.

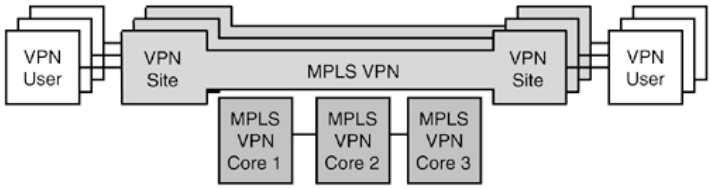


Fig. 3.4 Modelo con Internet

En este caso se puede observar en la figura 3.4, que a veces se necesita vincular diferentes redes de proveedores para poder ofrecer el servicio VPN a usuarios de distintas “cores”. Como en los casos anteriores, las redes “base” siguen siendo invisibles para las VPNs, ya que no existe relación con los “cores”. En realidad, para los usuarios no supone ningún cambio que sus datos atraviesen una o múltiples backbones. Aunque sí supone cierto riesgo entre las diferentes redes core.

Tanto en los casos tratados, como en el resto de posibles e imaginables, debe existir cierta confianza en que los bloques-módulos vecinos son seguros. De todos modos, se deben tomar precauciones para evitar que se cuelen ataques de DoS de una red core a otra. Por la misma razón por la que se coloca un firewall/NAT en las conexiones con extranets. Aunque entre módulos no vinculados no existe ningún tipo de peligro, entre aquellos que sí lo están se deben tomar las precauciones pertinentes, algunas de las cuales se tratarán en la sección 3.3.

3.2. Amenazas a MPLS VPN

Para cualquier red existe un gran surtido de amenazas que pueden hacer temblar los cimientos de su infraestructura. Para ATM pudimos ver como tanto las PVCs como los mensajes de señalización podían ser atacados. Y justamente por eso ATM Forum creo las especificaciones que se trataron.

Para MPLS también existen muchos puntos peligrosos, puntos calientes, por donde los “chicos malos” pueden tener alguna posibilidad de entrar. Las amenazas son prácticamente las mismas, aún cambian los elementos. Así pues, podemos decir que las mayores amenazas son las siguientes:

- Observación de las conexiones para envíos de rutas y entiquetas, entre el PE y CE, y cores diferentes.
- Ataque DoS y DDoS a los PEs
- Falsificación de etiquetas y direcciones IP
- Lectura de la información de los mensajes internos del core
- Ataques entre VPNs conectadas a través de una extranet
- Ataques desde Internet

Como en el caso de ATM, los ataques de spoofing y DoS son los más comunes. Y, por lo tanto, serán los tipos de ataques que más se referenciarán durante la siguiente sección, dónde se observarán las soluciones intrínsecas MPLS y las soluciones a los problemas que se presentan. De todas maneras, en el anexo B, se pueden ver los puntos calientes de MPLS, y una zona de consulta para entender mejor la siguiente sección.

3.3. Seguridad en MPLS

La mayoría de los análisis sobre seguridad que corren por las bibliotecas e Internet, tienen como objetivo comparar puntos concretos de MPLS con ATM. Estos requisitos que se revisan a MPLS son:

- Separación de espacio de direcciones
- Separación entre VPNs
- Resistencia a los ataques
- Ocultación del core
- Resistencia a ataques spoofing

Hacer el análisis de estos requisitos y determinar si MPLS es segura y si alcanza el nivel de ATM no llevaría mucho tiempo. Observando las características de MPLS, se pueden intuir las respuestas. Su diseño se creo intentando responder afirmativamente a la pregunta: ¿Cumple MPLS el requisito de …?

Durante este último capítulo, abriremos aquellas puertas que los investigadores de esta tecnología no habían abierto hasta hace poco. En él se tratarán características del RFC 2547bis y se intentará dar una valoración más cercana a la realidad.

3.3.1. Separación entre VPNs

Una de las facilidades que aporta MPLS a los clientes de las redes backbones, es que pueden seguir utilizando su rango de direcciones sin ningún problema. MPLS, mantiene separados los rangos de direcciones de las VPNs y el core a través de un formato de empaquetamiento llamado VPN-IPv4.

Como se explica en el Anexo E, este estándar permite la distinción de direcciones entre VPNs añadiendo a los 4 bytes de las direcciones de IPv4 (o los 16 de IPv6), 8 bytes llamados *Route Distinguisher* (RD). Lo que permite una gran cantidad de repeticiones de direcciones sin solapamientos. Estos identificadores, son difundidos y asignados por el multiprotocolo BGP (MP-BGP), que es el único que realiza esta tarea. De esta manera, se asegura que no existen dos identificadores RD idénticos en toda la red.

Por otro lado, a cada VPN se le asigna una instancia o tabla VRF (*Virtual Routing and Forwarding*). Por su parte, cada PE mantiene estas tablas separadas las unas de las otras, con lo que la información sobre las direcciones de cada VPN y las direcciones de los PEs conectados a los CEs de su misma VPN, permanecen ocultas. Únicamente la PE de cada VPN tiene conocimiento de las direcciones que la forman, y ningún otro dispositivo de la red u otras VPNs tienen acceso a esa información.

3.3.1.1. Separación de tráfico

El tráfico de una VPN se divide en tráfico de plano de control y tráfico de plano de datos. El plano de control es el tráfico originado y terminado en el mismo core; y por su parte, el plano de datos contiene el tráfico enviado desde las diferentes VPNs. Este tráfico es encapsulado y enviado de PE a PE añadiendo una etiqueta llamada LSP (*Label-switched Paths*).

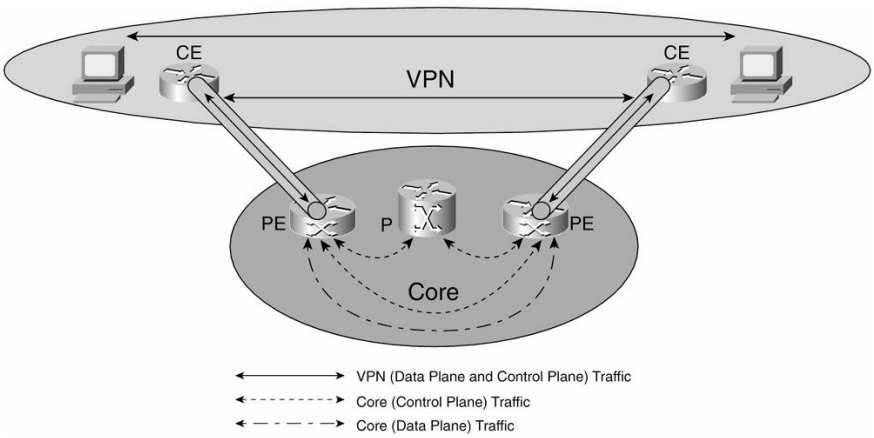


Fig. 3.5 Separación de tráficos

Como se puede observar en la figura 3.5, los diferentes tráficos quedan separados los unos de los otros. Por ello, todo el tráfico entre CEs resta oculto para el core.

Una simple demostración de que las VPNs se mantienen separadas, es la prueba que comenta Holly Xiao en su trabajo “Security Measurement on MPLS-VPN”. Para esta prueba se utilizaron: un P router, dos PEs de los que colgaban dos redes de cada una. Con ellas se formaban dos VPNs (VPN-A, VPN-B). La prueba es muy simple: enviar un ping de un terminal a otro.

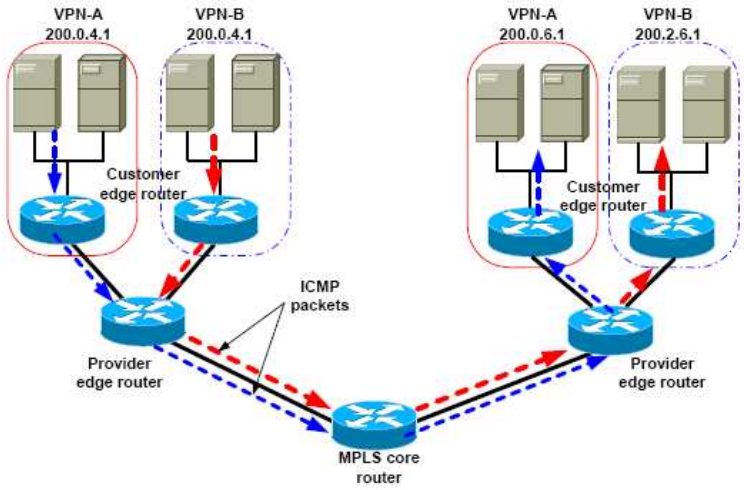


Fig. 3.6 Separación de VPNs

El la figura 3.6 se demuestra que incluso habiendo utilizado el mismo rango y las mismas direcciones, los paquetes ICMP llegan a su destino real.

Conociendo esto, podemos concretizar más y observar que la separación del tráfico, recibe diferente trato dependiendo del tipo de interfaz utilizada:

- Interfaz no-VRF: Este tipo de interfaz está asociada con una tabla de enrutado global. Por ello la decisión de envío se toma a partir de esta tabla y el paquete es tratado como un paquete IP normal. Este tipo de interfaz se encuentra en el core y en casos de vinculación de la red de servicios con Internet.

- Interfaz VRF: En este caso la decisión se basa en la información de la tabla de encaminamiento de la VRF. La separación de varias VPNs viene creada por la encapsulación de los paquetes con la cabecera VPN que le pertenece.

Con todo esto queda claro que:

- Con MPLS se consigue la separación de direcciones, tráficos y VPNs
- Se consigue tanto escalabilidad como seguridad ya que ni el core ni las diversas VPN son alcanzables entre sí
- Es imposible introducirse en otra VPNs que no sea la que se tiene asignada
- No se puede acceder desde el exterior al core amenos que se autorice a ello

3.3.2. Ocultación del Core

Éste es uno de los requisitos de seguridad más exigidos por los detractores de MPLS. ATM consigue ocultar el core, porque trabaja a nivel 2, mientras que MPLS lo hace a nivel 3. Sin lugar a dudas, la ocultación es un gran beneficio en la lucha contra los atacantes de redes. Poder ocultar la red, significa que los atacantes no tienen posibilidad de conocer direcciones internas que puedan ser atacas.

Para poder atacar un elemento interno de una red, primero se debe conocer su dirección. Y MPLS no rebela ninguna información sobre el core al exterior. El único elemento del que se puede poseer esa dirección es del PE (tratado un poco más abajo). Incluso conociendo o intuyendo la dirección de alguno de los elementos interiores de la red, MPLS trata a todos los mensajes llegados por una VPN como mensajes de esa VPN, y por lo tanto no circulan a otro lugar (ni a las direcciones internas del core, ni a otras VPN). Por lo que un ataque desde el exterior a cualquier elemento interno de la red es muy difícil de conseguir también en redes MPLS.

Como se ha podido notar, me he referido a la anterior opción de ataque desde una perspectiva exterior. En cuanto un ataque desde el interior, no existe capa o protocolo en particular que garantice la protección contra ataques internos. De alguna manera se podrán encriptar los datos, pero incluso en ATM es posible este tipo de ataques.

En cuanto a la revelación de información de las redes de los clientes a las PEs, ya hemos visto que la información únicamente queda almacenada en cada VRF con lo que ninguna otra VPN tendrá acceso a esa información. Anunciar esa información no compromete la seguridad de la red del cliente, porque la información conocida por el core es sobre rutas de la red y no información de host específicos.

Por lo que se ha explicado hasta el momento, existen dos maneras de atacar el core:

- Atacado directamente los routers PE
- Atacando los mecanismos de señalización

Es posible atacar a los routers frontera (PE) porque es la única dirección revelada al exterior. Esta información es revelada por el enrutado entre el CE y el PE. Esta operación puede ser ejecutada de dos maneras:

- Por enrutado estático: En este caso los routers PE son configurados estáticamente con la información de la red del CE; y los CEs son configurados también estáticamente apuntando hacia el PE u otras partes de la VPN (normalmente un router por defecto). La ruta estática puede apuntar a la dirección IP del router PE, o a la interfaz del router CE (por ejemplo, serial0). En la segunda de las opciones, el CE no necesita conocer ninguna de las direcciones IP en la red core, ni tan solo las direcciones del PE. Aunque esta opción tiene la desventaja de requerir una configuración estática más extensa, es ideal desde una perspectiva de red segura. En este caso es posible configurar un ACL (*Acces Control List)* en el PE. Con ello se puede bloquear todo el tráfico hacia su interfaz.

- Por enrutado dinámico: En todos los casos donde se utilizan protocolos dinámicos de enrutado (RIP, BGP, OSPF), cada CE necesita conocer por lo menos la identificación del router del PE, y por lo tanto almacena una destinación potencial para un ataque. En la práctica, los proveedores de servicio pueden limitar el acceso al PE aprovechándose del protocolo de encaminamiento, de las siguientes maneras:

  - Usar ACLs para limitar el acceso sólo a paquetes de enrutado y al puerto (o los puertos) del protocolo, enviados desde el CE
  - Cuando sea posible, configurar la autenticación Message Digest MD-5 para protocolos de enrutado. La autenticación MD-5 está disponible para BGP (RFC 2385), OSPF (RFC 2154) y RIP2 (RFC

2082). Esto previene el spoofing desde elementos del interior de la red del cliente que no sea el CE

- Cuando sea posible, se podría configurar parámetros del protocolo de enrutado para fortalecer la seguridad. Por ejemplo, se debería limitar el número de interacciones de enrutado. También se podría configurar un máximo nombre de rutas aceptadas por VRF. Esto ayudaría a asegurar que una VPN no pueda inundar el *provider-edge router* con demasiadas rutas. La utilización de Generalized TTL (Time-to-Live) Security Mechanism (GTSM, RFC 3682), en su caso sería una buena baza de seguridad que debería utilizarse en todos lo protocolos que lo soporten (incluso con el protocolo interno LDP – *Label Distribution Protocol*)

En resumen; no es posible introducirse de una VPN a otra. Y aunque el core revelase direcciones de sus PE a sus respectivos CEs, hemos podido ver que existen recursos para poder evitar un ataque. De todas maneras, y como veremos en la sección de ataques de spoofing y DoS, sigue siendo posible un ataque DoS aunque se reduzcan las posibilidades.

Al menos en lo que respecta al objetivo de este punto (ocultación del core), queda claro que se consigue, aunque como veremos más adelante, en opciones de uso de Internet, se deberá trabajar algo más para poder evitar intrusiones. En este caso, el uso de NAT ayudaría a asegurar la privacidad de los usuarios de las VPNs.

3.3.3. Resistencia a ataques

Para resistir a los ataques, MPLS utiliza filtrado de paquetes y no revelación de información del core. De esta manera, los ataques son mucho más complicados y obligan a los “chicos malos” a buscar alternativas.

Se ha podido ver hasta ahora que MPLS ofrece ocultación de las direcciones internas y del acceso a la tabla de enrutado global. Con la ayuda de los filtrajes a través de inclusión de ACL en los routers PE y la aplicación de diferentes configuraciones de seguridad en protocolos dinámicos de enrutado, se consigue una seguridad igualable a ATM y FR. En ambientes con acceso a Internet, la información revelada al exterior, si se siguen unos requisitos mínimos de seguridad, MPLS también puede estar a la altura.

Con la ayuda de la separación de VPNs, en caso de que se produjera un ataque, éste perjudicaría únicamente a los miembros de la VPN y no al resto de VPNs establecidas o al core. El único problema llegaría de la mano de ataques DoS que reducirían la capacidad de gestión de las PE, peligrando así los valores mínimos de QoS.

En ambientes de infraestructuras backbones múltiples, llegarían una serie de debilidades que no se encuentran en la opción de backbone monolítica. Este

tipo de debilidades y las alternativas de seguridad se expondrán más adelante de manera amplia. De todas formas, con una buena configuración y mantenimiento de la red, se consigue una resistencia de valores comparables con ATM y FR.

3.3.4. Spoofing

Este tipo de ataques puede afectar tanto a redes de nivel 2 como de nivel 3. Por ello todas las redes-backbones deben protegerse contra este tipo de ataques. Particularmente para MPLS se presentan dos alternativas de ataque para los “chicos malos”:

- IP spoofing: MPLS permite a sus clientes utilizar todo el rango de direcciones (de 0.0.0.0 a 255.255.255.255). Esto permite un gran margen de maniobra a los atacantes con este tipo de armas. La utilización de VRF, permite a MPLS retener este tipo de ataques en la VPN. Con ello se evita que puedan “saltar” a otras VPNs de la red. De todas formas, para este tipo de ataques, los investigadores consultados (normalmente de Cisco), piden a los administradores de las redes Cliente que utilicen refuerzos de seguridad, ya que sólo les afectará a ellos.

- Label spoofing: Dentro del core, los paquetes de diferentes VPNs se distinguen por la inserción de etiquetas. Un usuario malicioso de una VPN podría intentar crear su propia etiqueta (falsa) para entrar en el core. De esta manera podría infiltrarse en el tráfico de otra VPN. Por esta razón, cualquier paquete con etiqueta llegado de un CE es descartado por los PEs. Eso hace de este tipo de ataques simplemente imposibles.

Como MPLS dispone de la separación de VPNs este tipo de ataques quedan contenidos en las propias VPNs. Con lo que se puede decir que los usuarios de las VPNs (maliciosos o no), sólo se pueden atacar a ellos mismos. Con lo que no hay ningún riesgo para el core, ni el resto de VPNs.

3.3.5. DoS

Este tipo de agresiones son los más difíciles de contener. Cualquier protección existente hoy en día no asegura un 100% de fiabilidad, ya que hace es difícil encontrar una solución con las tecnologías actuales.

Este tipo de ataques pueden intentar afectar a MPLS sobreutilizando los siguientes recursos:

- Sobrecargando la línea en una red
- Excediendo la capacidad de envío de paquetes de un router

- Excediendo la capacidad de proceso de paquetes de un servidor

En general los ataques DoS están dirigidos a agotar uno de los siguientes recursos:

- Ancho de banda
- CPU
- Memoria

Este tipo de ataques suelen llegar desde Internet, aunque también se pueden colar por las VPNs. Entre la conexión de Internet y la de VPN, existe una gran diferencia de ancho de banda. Al consumir más ancho de banda Internet, en casos de repetición de paquetes, como en un ataque DoS, las VPNs reducen su capacidad, incluso llegando a la desconexión.

La única manera para el proveedor de solventar este tipo de ataques es sobretodo, disponiendo de un correcto posicionamiento de dispositivos, para poder solventar la demanda de recursos de ciertas zonas de la red. También es positivo hacer una correcta planificación de los anchos de banda y disponer de una buena política de QoS. A todo esto, se le debe añadir algunas de las opciones que ofrece MPLS para poder solventar este tipo de problemas.

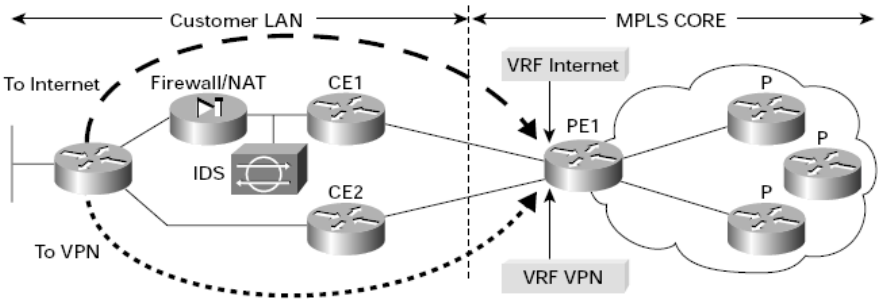


Fig. 3.7 Separación de VPN e Internet a dos PEs

La solución que se representa en la figura 3.7 es la más resistente a los ataques DoS. En la estructura se puede observar la partición de las conexiones de Internet e VPN para la red de un Cliente. Para cada conexión se dispone de un router CE. En el caso de la conexión a Internet, para facilitar la seguridad, la privacidad y la interoperabilidad se incluye un dispositivo IDS (*Intrusion Detection System*) para detectar accesos no autorizados o el uso incorrecto del sistema, y un firewall/NAT.

Como se puede observar, cada conexión apunta a una VRF distinta, y además en PEs distintas. Así, en caso de ataque a través de Internet, la VPN no es afectada de ninguna manera. El único punto negativo de esta solución, es el coste, ya que requiere de una gran inversión por parte de los Clientes.

Existen otras alternativas en que siguen utilizando las conexiones VRF por separado, pero en un mismo PE. Por otro lado, también existe la posibilidad de que la conexión de Internet pase de CE1 a CE2 antes llegar al PE. De esta

manera comparten una línea de acceso las dos VPNs, y se separan a través de subinterfaces creadas con VLAN o con links lógicos de Frame Relay. Otra opción más encaminada a MPLS sería el uso de una VRF para Internet, con lo que las dos VPNs restarían separadas a nivel lógico (opción mostrada presentada en la figura 3.8).

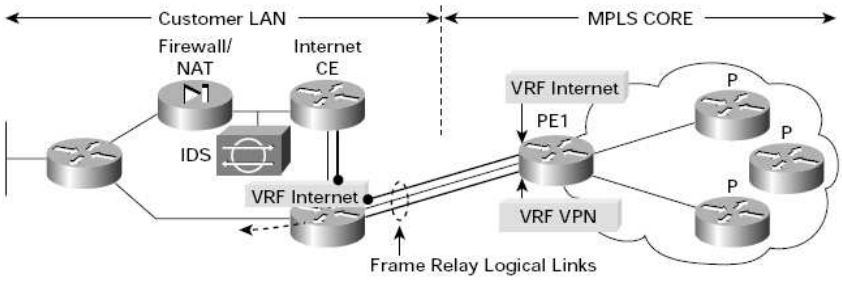


Fig. 3.8 Separación de VPN e Internet a un PE con VRF Internet

Estas alternativas tienen la ventaja de exigir un menor reembolso de los Clientes, pero también de reducir su resistencia ante ataques DoS. Como siempre, ante tantas opciones, los Clientes deben listar sus necesidades y amoldarse a las exigencias y al bolsillo.

Para aquellas empresas que tengan repartidas diversas sedes y necesiten Internet, la solución más barata es crear una vinculación Hub-and-Spoke (**Fig. 3.19**). Esta es una buena alternativa segura y más barata que la de crear este complejo sistema de conexiones en cada sede.

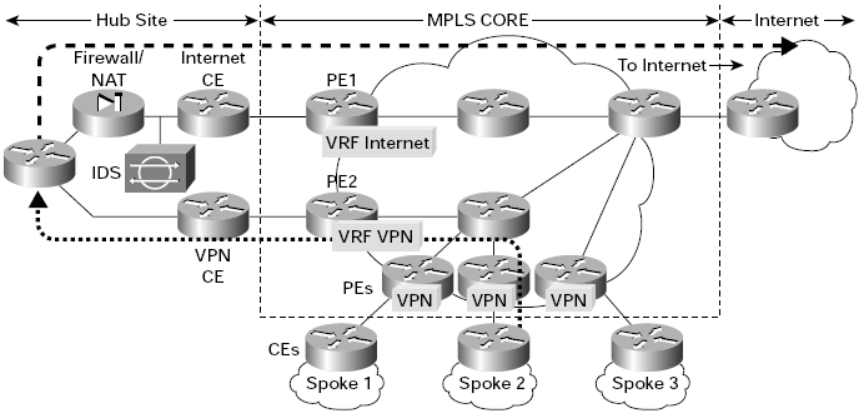


Fig. 3.9 Hub-and-spoke

La separación entre los tráficos de las diferentes sedes permanecen separadas, y todo el tráfico de las sedes (centrales o no) pasan por la sede denominada Hub. En este caso, la conexión de las sedes e Internet están en distintos PEs, pero uno sólo podría hacerse cargo de las dos conexiones.

3.3.5.1. Routers resistentes a DoS

Tecnológicamente estamos distantes de poder tener la capacidad de poder solventar con creces los efectos de un ataque DoS o DDoS. Haciendo boca, existe un router de Cisco llamado CRS-1 que da el primer paso. Este router tiene la peculiaridad de permitir separación de CPU y memoria completa. Con ello, la capacidad de procesamiento en un ataque se solventa con mayor facilidad, aunque, sinceramente, me gustaría saber como es de efectiva. Puede que de aquí a un tiempo lo podamos saber.

3.3.6. Extranet

Ya se ha repetido diversas veces que compartir elementos de red, o información, conlleva sus riesgos. De alguna manera u otra, las diferentes partes deben procurar dar el mínimo de información al resto. Otro punto a tener en cuenta es la compatibilidad de direcciones entre las distintas partes. Para este tipo de casos, siempre se puede optar por utilizar NAT para cada CE, o la ardua tarea de ponerse de acuerdo en cambiar las direcciones (mala opción!).

En el caso que nos ocupa ahora, estudiaremos un ejemplo donde dos clientes (VPN A y VPN B) comparten una recursos en una extranet). Como se puede observar en la figura 3.10, tanto VPN A como B, comparten sus rutas con la Extranet.

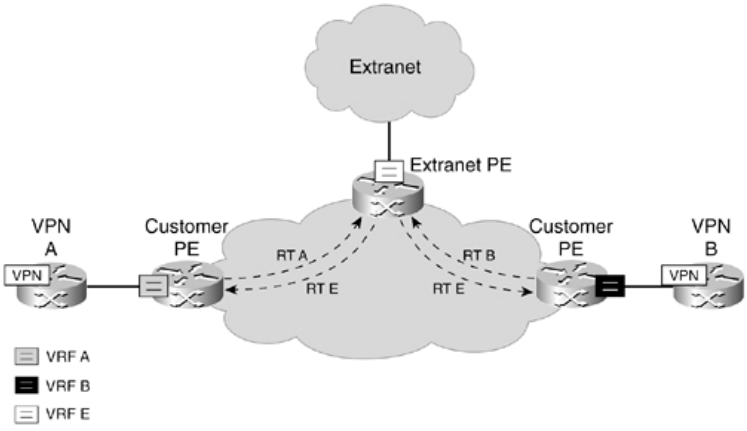


Fig. 3.10 Compartimiento de rutas

Lo que se debe evitar, es que B conozca las rutas de A y viceversa. Esto nos asegura que ningún ataque puede pasar de un lado al otro. Por ello, la mejor manera sería compartiendo la información a través de la extranet.

En el caso de que, por ejemplo, la VPN A se conectara a la extranet y conociera alguna dirección de VPN B, el envío de tráfico sería unidireccional. Sería unidireccional porque al haberse generado desde la extranet, B no conocería la dirección exacta de A. De todas maneras, un ataque unidireccional

también es posible. Se pueden enviar gusanos, por ejemplo, que no requieren más que un paquete.

Como siempre, no hay nada que evite la totalidad de los ataques, pero este tipo de consejos e implementaciones de MPLS ayudan a conseguirlo. De todas maneras, siempre es recomendable la utilización de firewalls para evitar entradas indebidas y una correcta actualización de los recursos software.

3.3.7. Internet

La “red de redes” es la mayor fuente de amenazas que existe para cualquier red conectada a ella. Es uno de los recursos indispensables para la mayoría de usuarios, empresas e instituciones; y por lo tanto no podía faltar en este trabajo.

Hemos podido ver que al compartir no se deben dejar puertas abiertas, y como veremos con Internet, esta es una tarea muy complicada.

Existen dos grandes opciones para ofrecer servicios de Internet en una backbone MPLS: Internet con una VRF e Internet con tabla de enrutado global. Esta última con dos opciones más: *Hop-by-hop* e *Internet-Free*.

3.3.7.1. Internet con una VRF

Esta es la manera más segura de poder ofrecer este servicio. Esta tarea acaba resultando como la creación de una conexión VPN como las que hemos estado viendo hasta el momento. Todas las conexiones hacía el proveedor de Internet se conectan al router PE de Internet directamente a la VRF (como se observa en la figura 3.11). Y todos los usuarios que quieran acceder sólo deben conectar con la VPN como hasta ahora.

El gran “pero” de este tipo de solución es que por cada prefijo reservado en un VFR, se requieren 3 veces más memoria que en una tabla global. Éste puede ser un gran *handicap* a tener en cuenta.

Los aspectos de seguridad de este tipo de infraestructura son:

- La separación entre VPNs se mantiene porque la Internet se considera como una VPN más
- Como el resto de VPNs, Internet no tiene acceso al core. Con lo que se preserva la seguridad de la red
- El core también es invisible desde Internet, ya que con el uso de la VRF se evita cualquier tipo de interacción
- Con todos estos argumentos, queda claro que: el spoofing de Internet a una VPN es imposible como entre VPNs

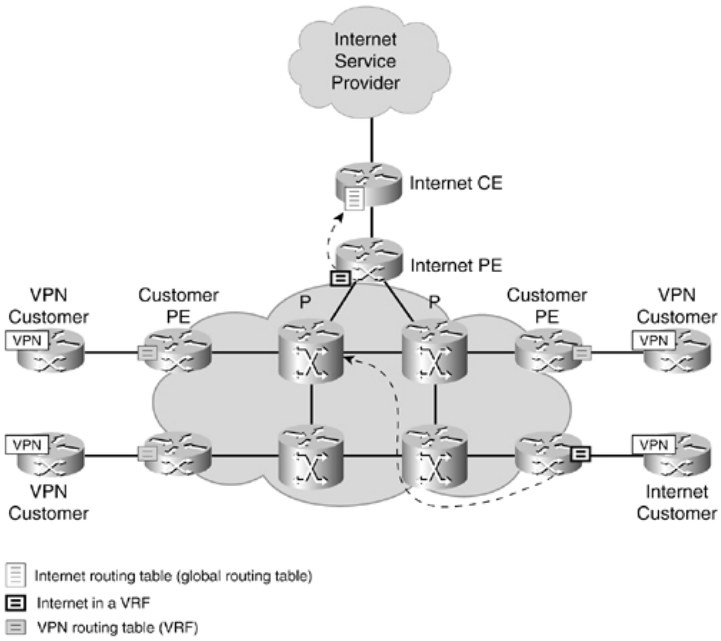


Fig. 3.11 Internet por VRF

3.3.7.2. Enrutado de Internet "Hop-by-hop"

Aunque la opción de utilizar la tabla VRF aporta gran seguridad a la red interior, también hace necesaria mucha reserva de memoria. Las tablas globales son la alternativa más directa pero necesitan otro tipo de mantenimiento y gestión, que como veremos con las dos próximas subopciones, repercutirá en la seguridad.

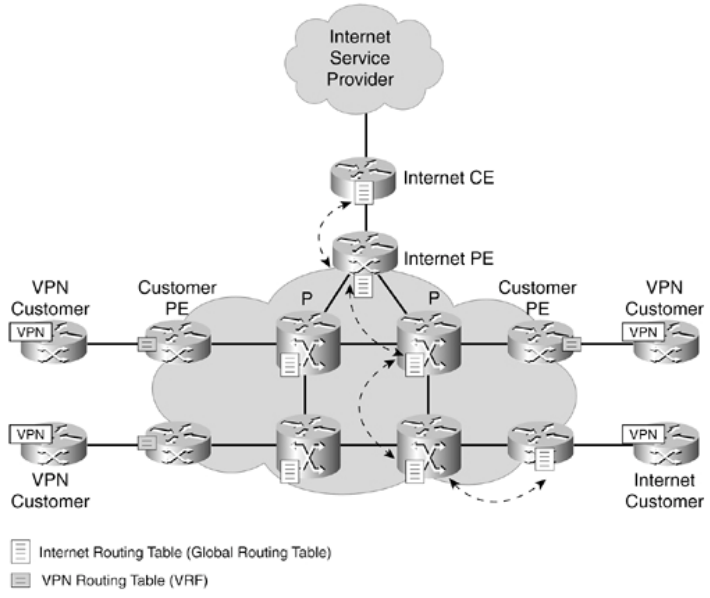


Fig. 3.12 Internet Hop-by-hop

Como se observa en la representación (**Fig. 3.12**), en este caso se combinan en el core las tablas VRF con las tablas globales de Internet. Por lo tanto se rompe a barrera de separación entre el core y el mundo exterior. Además, en la mayoría de casos en que se usa este tipo de infraestructura, tanto los PEs como los Ps, almacenan la tabla completa de rutas de Internet.

Como se puede intuir, no se aplica una de las grandes reglas de seguridad mantenidas hasta el momento: la ocultación del core. En este caso, es accesible desde Internet por defecto. Desde el punto de vista de seguridad, existen dos aspectos a tener en cuenta en los routers:

- Accesibilidad de Internet a un router: Los paquetes originados en Internet pueden ser dirigidos a un router. Esto expone al router a ataques directos y debería evitarse en la escala de lo posible.

- Accesiblilidad de un router a Internet: Un router puede alcanzar elementos de Internet, y esto permite que se puedan establecer conexiones. Este tipo de situaciones pueden provocar los ataques desde Internet ya que, al poder alcanzar Internet, los atacantes pueden establecer conexiones *two-way*.

Una de las maneras que encontraron los proveedores de servicios para resguardarse de estos ataques, era disponer de ACLs en la frontera del core para controlar los puertos de acceso. Aunque, existen otras maneras para evitar esto como por ejemplo: no anunciando las rutas interiores al exterior o usando un espacio de direcciones privadas en el core.

La accesibilidad de este tipo de modelos, obliga a la utilización de medidas de contención alrededor de toda la frontera de la red, como si de una fortaleza se tratara. Se deben evitar los accesos al interior de la red, que pudieran amenazar la privacidad de las VPNs.

3.3.7.3. Enrutado de Internet-Free

Este modelo pretende combinar lo mejor de cada uno de los anteriores. Por eso, utiliza tablas globales e intenta evitar el acceso desde el exterior limitando el número de tablas de enrutado de Internet.

Se observa claramente en la figura (**Fig. 3.13**) como únicamente el PE del CE del usuario de Internet, y el PE de Internet contienen la tabla global. Los Ps no almacenan ninguna información de nuevo. Por ello los routers P utilizan un protocolo de enrutado interior como IGP (Interior Gateway Protocol) a diferencia del modelo anterior que tenía que usar iBGP.

Evaluemos la accesibilidad a/de los routers en este modelo:

- Accesibilidad de Internet a un router: Las PEs almacenan las tablas globales, esto hace que puedan enviar y recibir todo el tráfico. Si les llega un paquete dirigido a un P, gracias a IGP consiguen enviar el paquete al correspondiente P. Por lo tanto existe accesibilidad.

- Accesibilidad de un router a Internet: Como los routers P no guardan información sobre Internet, estos no pueden alcanzar el exterior. Por lo tanto no puede existir una conexión *two-way*, y se convierte en un posible ataque unidireccional.

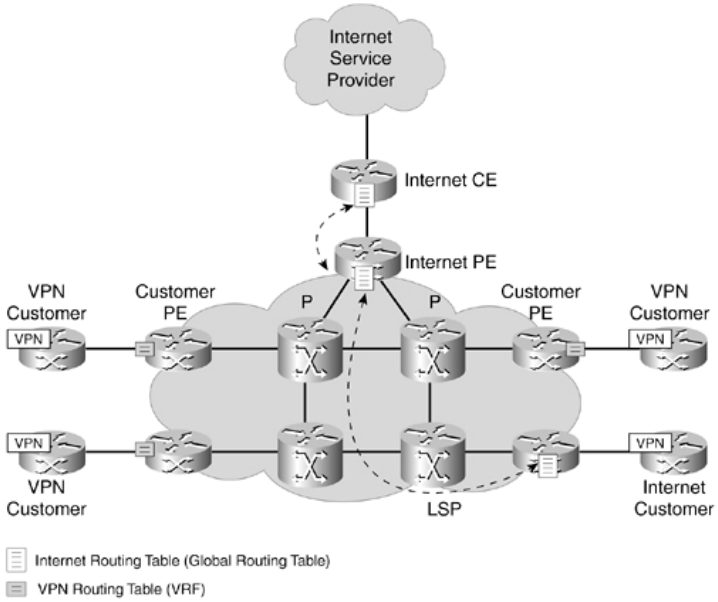


Fig. 3.13 Internet-Free

Como en los modelos anteriores, las VPNs no pueden ser atacadas directamente desde Internet, y la separación de VPNs y del core permanece intacta. La única amenaza es la posibilidad de un ataque DoS que pueda tener algún efecto sobre la disponibilidad de algunas VPNs.

Como ocurre en el caso anterior, es aconsejable cubrir la frontera de la red con ACLs para evitar, en la medida de lo posible, los accesos indeseados.

3.3.8. Inter-AS

Inter-AS es la agrupación de diferentes ASs para crear una misma backbone. Este tipo de solución se describió a partir del RFC 2547bis, y se diseñaron 3 modelos diferentes (A, B y C). Miremos pues de buscar sus puntos débiles y ver las posibles soluciones que existen.

3.3.8.1. Modelo A

Al “modelo A” también se le conoce como: *VRF-to-VRF Connections at the AS Border Routers*. Éste es el modelo más simple de los tres, y utiliza interfaces o

subinterfaces entre ASBRs (*Autonoms System Border Routers*) para mantener las VPNs separadas. Para ello, cada ASBR debe guardar un VRF por cada VPN compartida, como se muestra en la Figura 3.14.

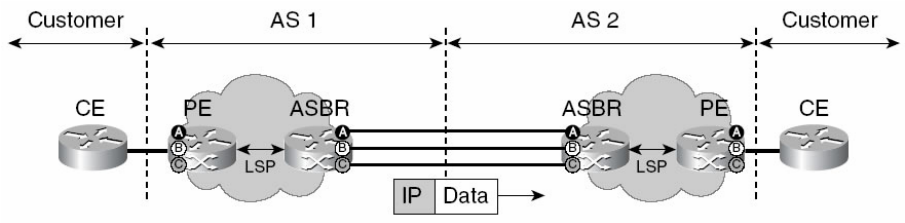


Fig. 3.14 Modelo A

Una de las grandes ventajas de este modelo es que no necesita casi ningún retoque respecto al modelo monolítico, ya que las conexiones establecidas entre ASBRs se asemejan a las creadas entre PEs y CEs. A consecuencia, hay una estricta separación entre VRFs. Esto hace imposible el ataque por spoofing, porque no se aceptan paquetes etiquetados del otro ASBR y los cores permanecen ocultos entre ellos. Por el contrario, crea un gran problema de escalabilidad ya que por cada VPN, se debe guardar un VFR y la necesidad de una nueva subinterfaz en cada ASBR.

Desde el punto de vista de seguridad, estos son los dos puntos a vigilar:

- Desconfiguración accidental en el ABSR: Éste es el mismo riego que existe para una red MPLS única, y también para las redes ATM y Frame Relay. Y no es más que la interconexión por equivocación de VPNs, con el consecuente riesgo de intrusión.

- Routing: Como ocurre con un PE común, es aconsejable el uso de MD5 para el intercambio de rutas entre ASBRs. De la misma manera, también es importante delimitar el número de prefijos de cada VRF para evitar que se pueda desbordar la memoria, porque una VPN anuncia demasiadas rutas.

3.3.8.2. Modelo B

A este modelo se le conoce por: *EBGP Redistribution of Labeled VPN-IPv4 Routes from AS to Neighboring AS*. Su particularidad es que elimina la necesidad de utilizar (sub-)interfaces para compartir VPNs. Una simple interfaz es necesaria para este cometido. Para conseguir la distinción entre los paquetes de datos de cada VPN, se añade una etiqueta a cada paquete. Estas etiquetas pueden ser configuradas manualmente, o mediante el uso del multiprotocolo MP-eBGP (*exterior BGP*). Con este multiprotocolo se pasan las rutas VPN entre ASBRs, y se asignan las etiquetas para ser utilizadas por cada prefijo VPN (ilustración de este modelo en la figura 3.15).

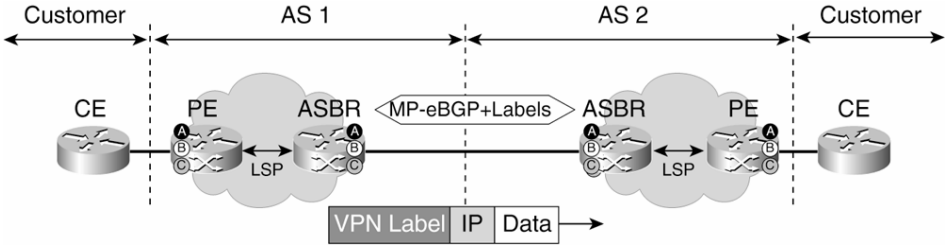


Fig. 3.15 Modelo B

El funcionamiento de este modelo se puede explicar claramente observando los planos de control y de datos. En lo que respecta al plano de control, se utiliza una simple instancia de MP-eBGP, intercambiando todas las rutas VPN-IPv4 junto con los parámetros requeridos (RD, etiqueta, etc.). Por otra parte, en el plano de control, todos los paquetes de VPN son etiquetados para distinguirlos los unos de los otros. En este modelo, el ASBR necesita conocer todas las rutas VPN intercambiadas como ocurre en el modelo A, pero en este caso utilizando sólo una interconexión.

En aspectos de seguridad, el plano de control, al utilizar un protocolo dinámico para el intercambio de las rutas, se debe utilizar algún tipo de autenticación como MD5. También se pueden considerar aspectos como: fijar un número máximo de rutas por ASBR y por VRF, controlar de la velocidad de anuncios para evitar sobrecarga de la CPU, filtrar de prefijos, descartar rutas IP, etc. Con estas medidas, se puede determinar que el plano de control tiene un nivel de seguridad comparable al del modelo A.

Por otro lado, en el plano de datos se comprueba la etiqueta de cada paquete, para verificar que realmente se haya asignado en el plano del control. Por lo tanto, es imposible introducir etiquetas falsas entre ASs. Sin embargo, no es posible comprobar que etiquetas son de cada ASs y podría colarse alguna etiqueta falsa. Para evitar este tipo de sucesos, se puede añadir un ASBR externo que compruebe-controle la validez de las etiquetas.

3.3.8.3. Modelo C

El modelo C, como en los casos anteriores, es conocido por otro nombre: *Multihop eBGP Redistribution of Labeled VPN-IPv4 Routes Between Source and Destination ASs, with eBGP Redistribution of Labeled IPv4 Routes from AS to Neighboring AS*. En este modelo se elimina la necesidad de almacenamiento de información sobre las VPNs en cada ASBR. Por ello, la información específica se propaga directamente entre el PE de ingreso de un AS y el PE de salida del otro AS. Para mejorar escalabilidad, se utilizan reflectores de la ruta (RRs).

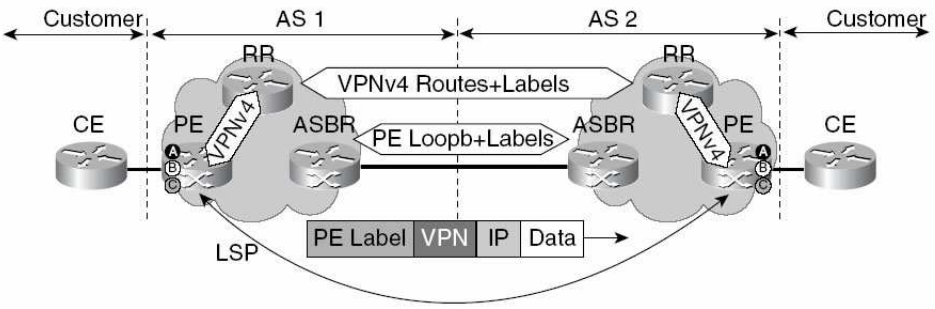


Fig. 3.16 Modelo C

Como se puede observar en la figura 3.16, se crea un conexión LSP (*Label Switch Path*) entre PEs (utilizando la dirección *loopback*). El trafico VPN, utiliza este LSP para alcanzar el otro AS. En lo que respecta al plano de datos, los ASBR actúan como Ps, ya que no tienen conocimiento del tráfico que circula. Lo mismo ocurre con el tráfico VPN ya que los paquetes circulan con la etiqueta VPN, pero también con la etiqueta PE de salida pertinente.

Para que este proceso de intercambio sea mucho más escalonado, como se ha dicho y se observa, se utiliza un reflector (RR) que hace de mediador. Con este dispositivo, las PEs de las dos ASs mantienen la conexión MP-BGP sólo con el RR de su propio AS. Los RRs, por tanto, son los que mantienen la correspondencia externa MP-BGP, y se intercambian la información específica VPN (VPN-IPv4 NLRIs, etiquetas, etc.) como ya pasara en el modelo B.

En lo que respecta a seguridad, no hace falta decir a estas alturas, que los intercambios de etiquetas (sobretodo por el intercambio de información de las PEs) entre ASs deben realizarse con una base de seguridad. La utilización de MD5, ayudaría a la preservar la seguridad de la información intercambiada. La utilización de filtros para rutas no adecuadas como IPs para ASBRs o VPN-IPv4, o el filtrado de prefijos entre RRs y ASBRs, son técnicas que asociadas con el control de la velocidad de intercambios, mejorarían el rendimiento del sistema y dificultarían los ataques.

Por otro lado, el aspecto favorable para la escalabilidad (el desentendimiento de los ASBR de la información de las VPNs), puede significar un retroceso en la seguridad. En este modelo, los ASBRs no controlan la información y por lo tanto puede colarse información no válida-falsa.

La consecuencia de este aspecto en la seguridad, puede crear un conflicto como el expuesto en la figura 3.17. En ella se muestra como una etiqueta es enviada desde *AS1* hacía *AS2* pero a una VPN que no tiene conexión entre ASs. Este tipo de situaciones pueden ser provocadas por una desconfiguración, y en caso de un ataque, éste sólo podría ser unidireccional. Es tal vez un aspecto de seguridad no tan alarmante como podría parecer, aunque evitable.

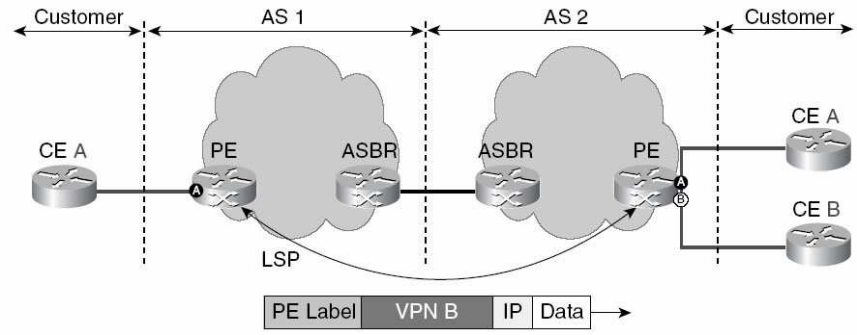


Fig. 3.17 Posible ataque en Modelo C

3.3.9. CsC

Como los modelos descritos antes, la arquitectura *Carrier's Carrier* (CsC) también se describe en el RFC 2547bis. Y no es más que un servicio backbone a proveedores de servicio.

La manera más sencilla de apreciarlo es tal y como se muestra en la figura (**Fig. 3.18**). En ella se muestra un primer nivel con un proveedor de servicio al que se le ha llamado "backbone carrier", y un segundo nivel donde aparece un proveedor que ofrece un servicio a sus clientes, pero que a su vez es cliente del "backbone carrier". A esta red se la llama "customer carrier".

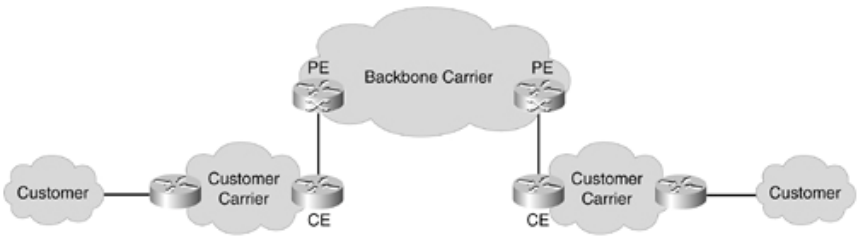


Fig. 3.18 Arquitectura CsC

Existen usos principales de este tipo de arquitectura:

- El *customer carrier* es un ISP: Para poder ofrecer este servicio, cada router del *customer carrier* debe guardar la tabla de referencias de Internet. Pero como hemos visto en el estudio de Internet, no es una buena idea que también lo tenga el *backbone carrier*. Por ello, una manera escalable de hacerlo es que el PE utilice VRFs. El uso de LSP extremo a extremo, reduce la lista de la tabla en los PEs a las direcciones de los puntos finales. De esta manera, los PEs y CEs se intercambian paquetes etiquetados y los prefijos correspondientes.

- El *customer carrier* es un proveedor MPLS VPN: En este caso, el PE del la backbone tendría que guardar una VRF con la información de cada cliente del *customer carrier*. Si el *backbone carrier* da servicio a muchos *customer carrier*, puede ser muy poco escalable. La solución es

intercambiar sólo direcciones *loopback IGP* con etiquetas, con lo que la backbone debe imponer una nueva etiqueta a los paquetes. De esta manera, los PEs de los *customer carrier* trabajan con MP-iBGP (*multiprotocol BGP interior*) directamente.
Con esta opción, los paquetes etiquetados por los *customer carrier*, son etiquetados también en el backbone. De esta manera se crea una vinculación que recuerda a los proveedores de servicios sencillos donde, el core no tiene ninguna conciencia de la información de las VPNs que le atraviesan (caso ilustrado en **Fig. 19**).

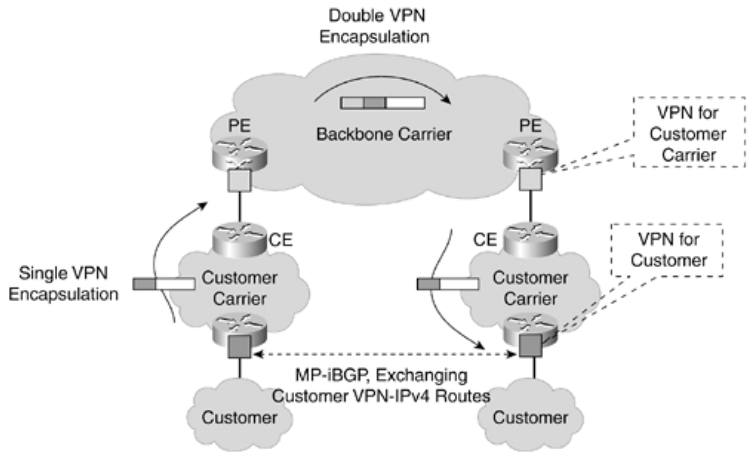


Fig. 3.19 VPN jerárquico

En cuanto a los aspectos de seguridad, podemos observar que en el plano de control, para configurar un IGP (*Interior Gateway Protocol*) con LDP o TDP, éste distribuye las rutas, mientras que LDP/TDP distribuyen las etiquetas para estas rutas. Por otro lado, el protocolo BGP combina las dos tareas. Por supuesto, este intercambio debe establecerse con autenticación MD5 (disponible para estos protocolos).

Como ya ocurriera en el modelo B de Inter-AS, las etiquetas son validadas por el plano de datosl, comparándolas con las obtenidas en el plano de control. Esto evita un posible ataque spoofing desde alguno de los *customer carrier*. De cualquier manera, se sigue el principio de separación de VPNs que evitan las propagaciones a otros enlaces virtuales.

3.4. Seguridad obligatoria

Durante todo este capítulo, hemos podido observar la gran variedad de soluciones que presenta MPLS. De cada una de las expuestas aquí, se han extraido algunos puntos conflictivos, tal y como nos pasaba con ATM.

Un punto en cuanto a seguridad que no se ha tratado aquí, es que relaciona el cliente con la proveedora de servicios. Siempre debe establecerse una relación

entre clientes o entre clientes y proveedores. Y tener en cuenta aspectos como: la autenticación, la seguridad a la entrada de sus redes, etc.

Estos aspectos, son a veces olvidados por los clientes. Estos, no deben dejar agujeros que puedan implicar a la VPN que tienen creada en la red MPLS. Por ejemplo, se comenta en el Anexo B.2.5, que la mala gestión de seguridad en el acceso wireless, puede causar la entrada de “chicos malos”. Esto, evidentemente, no es problema del proveedor de servicios. Como no es culpa del cliente, las desconfiguraciones de las rutas de los routers. Por ello, y haciendo referencia a una frase de Michael H. Behringer: no se pueden cerrar las puertas a cal y canto, y dejar las ventanas abiertas. Con lo que, cada administrador de red, debería crear una buena política de seguridad adaptada a su red. A partir de ahí, deberían cumplirse los objetivos marcados, y en el momento de compartir información con otras redes, conocer sus niveles de seguridad. Porque, aunque una red tenga un gran nivel de seguridad, si su homónima no lo tiene, pueden producirse situaciones desagradables.

CAPÍTULO 4. CONCLUSIONES

Último capítulo y el momento de evaluar los diferentes aspectos de este trabajo. Seguramente los comentarios que se ha hecho durante todas y cada una de las páginas que ya quedan atrás, han ayudado a responder la pregunta que se formulaba en la introducción: ¿Es MPLS tan seguro como ATM?. Aún así, en este capítulo se resumirán los puntos más importantes.

Antes de contestar a la pregunta, también se comentarán otros puntos relacionados con la seguridad y directamente con este trabajo. De esta manera, se completará un estudio dónde se han evaluado dos tecnologías y un punto en común entre las dos: la seguridad.

4.1. Recopilación de información

Sinceramente, estoy muy extrañado de la poca importancia que se daba hasta hace bien poco en este tema. No existe una documentación amplia hasta el año 1999. La mayoría de autores, no tenían en cuenta los aspectos de seguridad en las redes que comentaban. Lo único que hacían, era hacer pequeños comentarios durante las explicaciones (si en algún caso explicaban algo).

Desde el momento que me ofrecieron este TFC, ya me dijeron que se trataba de un trabajo meramente teórico. Sinceramente, este trabajo no se hubiese podido acabar si no hubiese encontrado la bibliografía adecuada, y no ha sido fácil pues es escasa. Y esa escasez aumenta cuando se habla de ATM.

Los detractores de MPLS son muchos, o por lo menos se hacen ver. Por eso, existe documentación donde los entusiastas de MPLS, se defienden de las críticas de los “menos entusiastas”. Pero, sólo he encontrado un documento que se dedique exhaustivamente a criticar ATM. Pero desafortunadamente no he podido conseguirlo, ya que sus derechos fueron comprados por una empresa especializada, que pide unos 700 dólares por una copia. En el se descubren los puntos débiles de ATM, algo que me hubiese gustado leer.

Lo que he conseguido sobre ATM es muy poco comparado con la información que existe sobre MPLS, sobretodo gracias a Cisco. De todas formas, la información que se ha descrito en los capítulos anteriores y en los anexos, ya ayudan a hacer conclusiones.

4.1.1. Cisco, Cisco, Cisco

Si no hubiese sido por la documentación que Cisco publica a través de libros o documentos de prensa, la información respecto a MPLS hubiese sido escasa.

Aunque pueda parecer que se trata de un agradecimiento a esta compañía, no lo es. En realidad, con esto vengo a decir que, con la información dada por una compañía que es la principal proveedora de dispositivos MPLS, se hacen más difíciles las críticas. Sus autores no van a tirar piedras a su propio tejado, y la evaluación de sus propios sistemas siempre son favorables o cogen la excusa de que a otras tecnologías también les pasa.

Realmente la documentación de Cisco está muy bien, pero he hechado mucho de menos, documentación de ATM que critique o que hable sobre MPLS. Evidentemente, la información que Cisco ofrece en sus publicaciones, ha sido contrasta con otras (de menor nivel), y siempre han sido favorables. Pero, a falta poder evaluar MPLS en un laboratorio, un poco de contrastes seguramente habría aportado más contrastes al trabajo.

4.2. Balance entre seguridad y coste

Este es un punto que se ha comentado algunas veces durante el trabajo. Pero es un punto destacable en cuanto a seguridad porque, como se ha podido ver, mayor poder adquisitivo puede significar mayor tranquilidad.

Un caso de este tipo se trató en la evaluación de las posibilidades de proveer de un servicio de Internet a un cliente de la red (tratado en la sección 3.3.5). Según la opción que se escogiera, el cliente podía tener que desembolsar más o menos dinero.

En este tipo de casos dónde se pueden escoger diferentes alternativas, se debe escoger la que mejor se adapte a las necesidades de la red. Por lo tanto, una política de seguridad de la red, puede ayudar a escoger la alternativa más conveniente. Evidentemente, también se debe mirar el bolsillo y escoger lo que la cartera.

No existe ni la red ni la tecnología que nos garantice un 100% de efectividad. Por lo tanto, a veces se deben tener en cuenta los riesgos que representa la utilización de una tecnología u otra, y si las pérdidas que puede provocar un ataque son asumibles.

Por lo tanto, en el momento de escoger una tecnología u otra se deben evaluar 3 puntos fundamentalmente:

- El coste de la operación
- El nivel de seguridad y los requisitos explicados en la política de seguridad de la empresa
- Evaluación de pérdidas asumibles por el uso de cada tecnología

4.3. ¿Es MPLS tan seguro como ATM?

En la sección 3.3, se presentaron los requisitos que debía alcanzar MPLS, y que han sido evaluados entra otras cosas. Estos puntos, se resumen en la siguiente tabla, comparándola con ATM:

Tabla 4.1. Tabla de requisitos de seguridad evaluados

Requisitos evaluados	ATM	MPLS
Separación de espacio de direcciones	Sí	Sí
Separación entre VPNs	Sí	Sí
Resistencia a los ataques	Sí	Sí
Ocultación del Core	Sí	Sí
Resistencia a ataques spoofing	Sí	Sí
Seguridad en multicast	Sí	En proceso

Como se muestra en la tabla 4.1, MPLS es tan seguro como ATM. Aunque ya se hayan evaluado estos puntos, vamos a ver un resumen de las razones por las que es así.

4.3.1. Separación entre VPNs y del espacio de direcciones

Las dos tecnologías pueden ofrecer estos servicios a sus clientes, aunque no lo hagan de la misma manera. En el caso de ATM, al trabajar en el core a nivel 2, y las VPNs lo hacen a nivel 3 con lo que, la información de las VPNs circula separadamente. En el caso de MPLS, esta tarea se hace a nivel lógico gracias a las VRFs que mantiene separadas las direcciones de los diferentes clientes del PE. Por las mismas razones, las dos tecnologías pueden ofrecer la posibilidad de utilizar todo el rango de direcciones a sus clientes.

Por ello, se puede decir, que no puede un usuario de una VPN atacar al tráfico de otra VPN porque los tráficos se mantienen separados e inaccesibles desde el exterior.

4.3.2. Resistencia a los ataques

Hemos podido observar, que es muy difícil atacar MPLS o ATM desde el exterior. Evidentemente, existen algunos puntos en que las dos tecnologías tienen algunos problemas si no se utilizan contramedidas.

ATM tiene algunos problemas en los switchs, porque trabajan a nivel 3 y si no se utiliza autenticación y filtraje de paquetes, pueden padecer ataques (por ejemplo de telnet). En cuanto a MPLS, vimos que existían problemas para algunas de las alternativas de ofrecer Internet a través de la red de servicios. Estos problemas de intrusión por la utilización de tablas globales en la frontera o en todos los puntos del core. La solución que comentamos era la utilización de ACL en toda la frontera, para filtrar las entradas indeseadas (caso tratado en el 3.3.7).

Algunas veces (por ejemplo en el caso anterior), se destacaba que los ataques sólo podía ser unidireccionales. Esta situación evidentemente es una ventaja respecto a la posibilidad de un ataque bidireccional, pero sigue siendo un ataque. Tanto MPLS como ATM pueden padecer este tipo de ataques (cualquier tecnología VPN lo puede sufrir), y son un punto a evaluar en el momento de escoger un tecnología y un sistema de seguridad (como se ha explicado en la sección 4.2).

4.3.3. Ocultación del core

Como ATM trabaja a nivel 2, el core se mantiene oculto porque el tráfico de usuario trabaja a nivel 3. En el caso de MPLS, los elementos del interior del core no conocen ningúna información sobre las VPNs de los usuarios. Además, no se rebela al exterior ninguna información sobre los elementos que componen el core. La única información que sí es conocida, es la dirección del PE conectado al CE del cliente. Igualmente, esta información no puede ser utilizada por un atacante para introducirse en el core.

Como siempre, una buena configuración, puede controlar los ataques.

4.3.4. Resistencia a ataques spoofing

Tanto MPLS como ATM, impiden los ataques de spoofing. En ATM no se puede hacer un ataque de este tipo, ya que conocer los identificadores VPI/VCI para atacar otra VPN es muy difícil. Aparte, la utilización de autenticación aún imposibilita más esta operación.

En MPLS, si se consigue atacar una VPN, este ataque siempre permanecería en el interior de la VPN atacada, jamás se podría saltar a otra VPN. Por lo tanto, las dos tecnologías resisten a este tipo de ataques.

4.3.5. Seguridad en multicast

Este es uno de los puntos más destacados en las críticas de los detractores de MPLS. ATM, soporta multicast y asegura sus tráficos en cambio dicen que MPLS no puede hacerlo porque le cuesta crear flujos de este tipo, y dejan agujeros en la seguridad.

La propuesta de seguridad en multicast aún se está haciendo. El grupo de trabajo de L3VPN de IETF, trabaja en el para que esas críticas no sean tal.

4.3.6. Ataque desde el interior

Como último punto, cabe destacar que ninguna de las tecnologías basadas en VPN puede evitar un ataque desde el interior. Tanto en ATM como en MPLS, la solución es la encriptación y autenticación del tráfico de control ayuda a ello.

Los usuarios que no confíen en la seguridad del core pueden utilizar IPsec para sus conexiones, que ayuda a asegurar la confidencialidad de la información.

Como se ha podido observar, MPLS y ATM tienen un nivel parecido. Digo parecido, porque jamás se puede estar seguro sin un estudio intensamente exhaustivo (algo que sin pruebas de laboratorio es difícil). Pero, yo le doy un plus a MPLS por la mayor versatilidad y facilidad a la hora de actualizar el software o elementos de la red. Este punto se debe tener en cuenta porque en casos de ataques nuevos, una actualización rápida y ágil siempre ayuda a defenderse.

Por lo tanto: ¿Es MPLS tan seguro como ATM?. Mi opinión es que sí. E incluso MPLS un poco más porque es más fácil emplear una actualización.

BIBLIOGRAFÍA

- **Bibliografía sobre seguridad**

[1]. James F. Kurose, Keith W. Ross, *Redes de computadores. Un enfoque descendente basado en Internet*, Pearson Addison Wesley, 2004.

[2]. Rolf Oppliger, *Security technologies for the world wide web*, Artech House, 1999

[3]. William Stallings, *Network Security Essentials. Applications and standars*, Student Resources

[4]. James D. McCabe, *Network analysis architecture, and design*, Morgan Kaufmann Publishers

[5]. Num. 5 *Concections*, AT&T, 2002

[6]. *Cortafuegos: la major defensa*, Iworld, www.idg.es/iworld

[7]. Saulo Barajas, *Seguridad en BGP,* Universidad Carlos III de Madrid

- **Bibliografía sobre VPN**

[8]. Marco Carugi, Jeremy De Clercq, *Virtual Private Networks services: scenarios, requirements and architectural constructs from a standardization perspective,* IEEE Communications Magazine, Junio 2004

[9]. Tomori Takeda, Dimitri Papadimitriou, *Layer 1 Virtual Private Networks: Dirving Forces and Realization by GMPLS,* IEEE Communications Magazine, Julio 2005

[10]. Paul Knight, Chris Lewis, *Layer 2 and 3 Virtual Private Networks: Taxonomy, technology, and standardization efforts*, IEEE Communications Magazine, Junio 2004

[11]. Chris Metz, *The latest in Virtual Private Networks: Part I*, IEEE Internet Computing, Enero-Febrero 2003

[12]. Chris Metz, *The latest in Virtual Private Networks: Part II*, IEEE Internet Computing, Junio 2004

[13]. Tomori Takeda, Ichiro Inoue, Raymond Aubin, Marco Carugi, *Layer 1 Virtual Private Networks: Service concepts, architecture requirements, and related advances in standardization*, IEEE Communications Magazine, Junio 2004

[14]. Jun Kyun Choi, Dipnarayan Guha, Seng Kyoun Jo, *Framework of PCEMP based Layer 1 Virtual Private Network*, Network working group, Julio 2005

- **Bibliografía sobre ATM**

[15]. Thomas D. Tarman, Edward L. Witzke, *Implementary Security for ATM Networks,* ArtecHouse Publishers, 2002

[16]. Maryline Laurent, Ahmed Bouabdallah, Christophe Delahaye, *Secure Communications in ATM Networks,* Project Scan, 2000

[17]. David Ginsburg, *ATM: Solutions for Enterprise Internetworking*, Addison-Wesley, 1998

[18]. David Ginsburg, *ATM: Solutions for Enterprise Internetworking*, Second Edition, Addison-Wesley, 1999

[19]. Rainer Händel, Manferd N Huber, Stefan Schröder, *ATM Networks: Concepts, Protocols, Applications,* Third Edition, Addison-Wesley, 1998

[20]. Csaba Simon, Attila Török, *ATM Security with Firewalls,* High Speed Networks Laboratory, Department of Telecommunications and Telematics, Technical University of Budapest, 2000

[21]. Mohammad Peyravian, Thomas D. Tarman, *Asynchronous Transfer Mode Security*, IEEE Network, Mayo-Junio 1997

[22]. Vijay Varadharajan, Rajan Shankaran, *Security for ATM Networks*, Distributed System and Network Security Research Unit, Dept of Computing, University of W. Sydney, Nepean, IEEE 1997

- **Bibliografía sobre MPLS**

[23]. Tiziano Tofoni, *MPLS: Fondamenti e applicazioni alle reti IP,* Editore Ulrico Hoepli Milano, 2003

[24]. Jesús García tomás, josé Luis Raya Cabrera, Víctor Rodrigo Raya, *Alta velocidad y calidad de servicio en redes IP,* RA-MA Editorial, 2002

[25]. Chuck Sameria, *RFC 2547bis: BGP/MPLS VPN Fundamentals,* Juniper Networks, 2001

[26]. Joël Repiquet, *Keep it Simple with BGP/MPLS Virtual Private Networks,* LambdaNet, Mayo 2002

[27]. Cisco MPLS Controller Software Configuration Guide, Setiembre 2003

[28]. Holly Xiao, *Security Measurement on MPLS-VPN,*

[29]. Ivan Pepelnjak, Jim Guichard, Jeff Apcar, *MPLS and VPN Architectures, Volumen II : Master the latest MPLS VPN solutions to design, deploy, and troubleshoot advanced or large-scale networks,* Cisco Systems, 2003

[30]. Comparing MPLS-Based VPNs, IPSec-Based VPNs, and a Combined Approach, Cisco Systems, 2004

[31]. Michael H. Behringer, Monique J. Morrow, *MPLS VPN Security,* Cisco Systems, Junio 2005

[32]. M. Behringer, *Analysis of the Security of BGP/MPLS IP VPNs,* Octubre 2004

ANEXO A. LOS FIREWALLS

Este anexo, es una extensión directa del 1.2. Se explican los diferentes tipos de firewalls existentes, y sus características más destacadas.

A.1. Firewalls

La figura A.1, nos servirá como punto de partida para entender los diferentes tipos de firewalls existentes hoy en día.

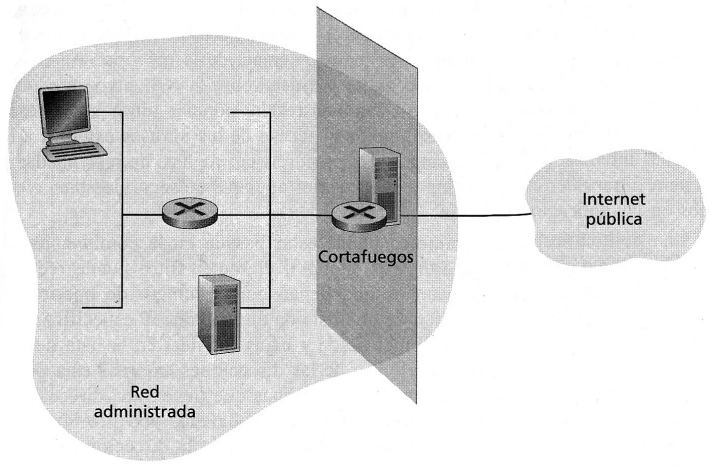


Fig. A.1 Red administrativa con cortafuegos

Como ya se indica en la sección 1.2, existen cuatro tipos de firewalls: de filtrado de paquetes, pasarelas de nivel de aplicación, Inspección multinivel de estados y *Circuit Level Gateways*. Así pues, empecemos.

A.1.1. Filtrado de paquetes

El filtrado de paquetes (*Packet-filtering Firewall*), se realiza analizado las cabeceras de los datagramas, lo que significa que se trabaja a nivel de red (**Fig. A.2**). Después de esta lectura, se observan las reglas de filtrado establecidas y se actúa según la política de seguridad de la red. Algunas de las reglas de filtrado más utilizadas se basan en los siguientes puntos:

- Direcciones IP origen y destino
- Puertos TCP o UDP origen y destino
- Tipo de mensaje ICMP (*Internet Control Message Protocol*)
- Datagramas de inicialización de la conexión utilizando los bits TCP SYN o ACK

Se pueden crear distintas reglas de filtrado, e incluso combinar algunas de las indicadas arriba. De esta manera se pueden hacer reglas como: filtrado todas las conexiones *Telnet* (TCP 23), de las conexiones UDP a una dirección IP, etc.

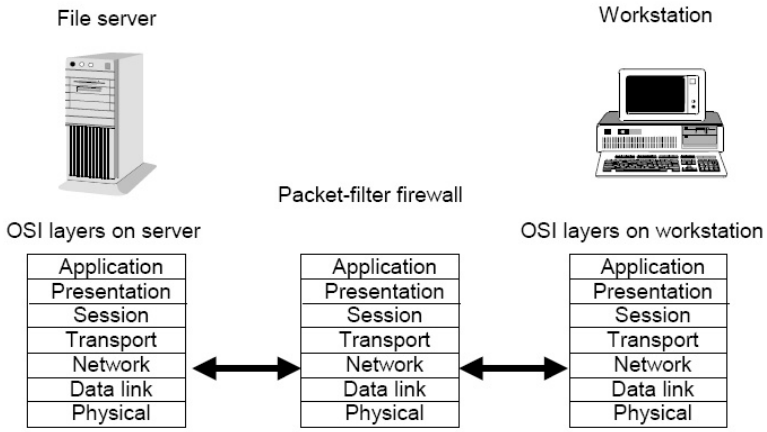


Fig. A.2 Packet-filtering Firewall

Una de las reglas más estrictas es la de no dejar pasar ningún tipo de tráfico; aunque es evidente que una conexión hacia el exterior debe hacerse servir más que para no utilizarla. Por lo tanto se suele dejar salir tráfico a unos usuarios en concreto o únicamente a unas IP destino establecidas (como las de una posible sede de esa misma empresa).
Habitualmente las grandes empresas bloquean los segmentos UDP. La desventaja de esta solución es que también bloquean todas las aplicaciones de difusión de audio y vídeo. También se suele bloquear cualquier conexión de *Telnet* para que cualquier usuario malicioso no pueda cambiar información del host o adquiera cualquier tipo de información importante.

Otra política de filtrado, puede combinar direcciones IP y puertos. Se puede dejar pasar por ejemplo, a un conjunto de direcciones del administrador dirigidas al puerto 23. Aunque esto tiene el problema de que un “chico malo” puede interceptar la dirección IP e infiltrarse utilizando una de las IPs disponibles.

El filtrado también puede basarse en el valor del bit TCP ACK. Este truco puede utilizarse cuando es necesario que clientes internos de la red puedan conectarse con servidores externo, pero impidiendo que los clientes externos se conecten a servidores internos. Esto es posible porque el valor del primer ACK en la inicialización de una conexión TCP tiene valor 0, y a partir del segmento de respuesta el valor es 1. Por lo tanto, cualquier segmento entrante con ACK con valor 0 es filtrado.

Como se puede observar, la gestión de un cortafuego puede llegar a ser muy compleja. Incluso así, no garantiza un 100% de eficacia. Por ejemplo, existen grandes dificultades para poder controlar el tráfico de fuentes inalámbricas. También existen algunos autores que destacan la vulnerabilidad de este sistema a los ataques *spoofing* (engaño-falsificación), aunque de todas maneras se pueden buscar ayudas para aumentar la seguridad.

A.1.2. Pasarela de aplicación

En algunos casos, las empresas necesitan que ciertas personas puedan acceder a servicios externos, o poder establecer un servicio Telnet. Este tipo de tareas restan lejanas de las posibilidades de un filtro como los proporcionados por los firewalls.

Para conseguir este tipo de seguridad selectiva existen las pasarelas de aplicación. Estos elementos, tienen la capacidad de mirar más allá de las cabeceras TCP/UDP/IP, y toman las decisiones basándose en los datos de la aplicación (como se ilustra en la **Fig A.3**).

Así pues, una pasarela de aplicación (*Application-level gateway*) es un servidor a través del cual deben pasar todos los datos de la aplicación a la que esta encomendado.

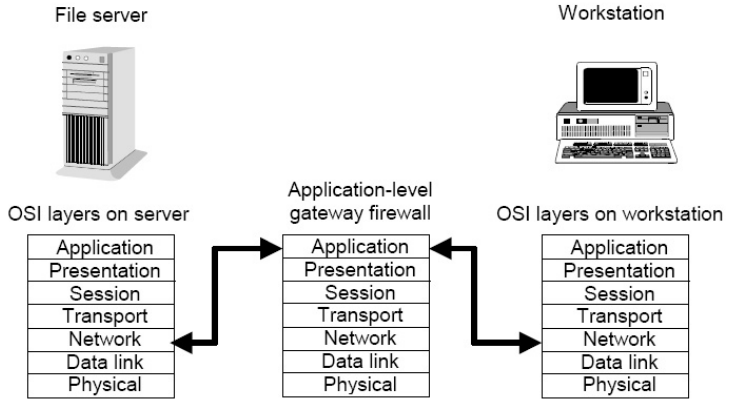


Fig. A.3 Application-level gateway

En una red como la que se puede observar en la figura A.4, existe un cliente de la red administrativa que quiere acceder (vía Telnet) a un servidor remoto.

El filtro (*Router y filtro* en la ilustración) está configurado para bloquear todas las comunicaciones Telnet excepto las que tengan su origen en un grupo reducido de la red. Todos aquellos intentos de conexión que tengan como origen algún miembro del grupo privilegiado, serán obligados a pasar por la pasarela de aplicación.

El cliente, en primer lugar, debe iniciar una sesión Telnet con la pasarela de aplicación. Para ello necesitará enviarle la identificación de usuario y la contraseña, para comprobar si tiene permisos para poder acceder a esa aplicación. Si no los tiene, la conexión se cierra. En cambio, si tiene permisos para poder establecer una sesión Telnet hacía el exterior, se continúa con los siguientes pasos:

1. La pasarela solicita al usuario, el nombre del servidor exterior con el que quiere realizar la sesión Telnet.

2. Se establece una sesión Telnet entre la pasarela y el servidor externo
3. La pasarela hace de intermediario entre el usuario y el servidor exterior

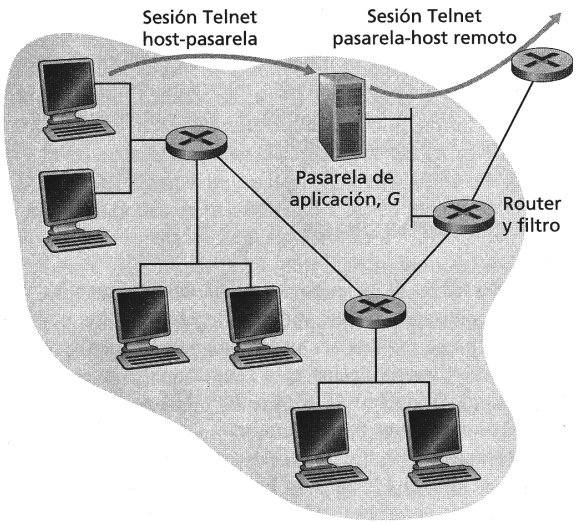


Fig. A.4 Red administrativa con Pasarela de aplicación

Puede observarse que todo el tráfico pasa por la pasarela, y ésta realiza la función de puente entre los dos puntos finales. De esta manera se evita que absolutamente nadie no autorizado pueda iniciar o continuar una sesión de Telnet.

Como ocurre con los firewalls, las pasarelas de aplicación, también presentan algunos problemas:

- Se necesita una pasarela de aplicación para cada aplicación; lo que genera una gran inversión por parte de las empresas.

- Las prestaciones se reducen si existen múltiples usuarios: Si diferentes usuarios autorizados utilizan la misma aplicación a la vez, el rendimiento y la velocidad de las conexiones se reducen.

- Se debe realizar una configuración extra: El software del usuario debe saber cómo contactar con la pasarela.

- El usuario debe conectarse obligatoriamente con la pasarela: Eso quiere decir que si la pasarela cae, no se pueden establecer comunicaciones Telnet hacia el exterior

A.1.3. Inspección Multinivel de Estados

La tecnología Inspección Multinivel de Estados (*Stateful Multi-Layer Inspection* - SMLI) busca combinar el buen rendimiento del filtrado de paquetes y la elevada seguridad a nivel de aplicación de las pasarelas. No se limita a

examinar los paquetes a nivel de red como hace el filtrado de paquetes, sino que los analiza a todos los niveles de la pila de protocolos, extrayendo la información relevante sobre el estado de la comunicación y de la aplicación (Ilustrado en la figura A.5). Aún así, esta solución es más rápida que la pasarela y no necesita que el usuario utilice un software específico.

Para cada conexión, el cortafuegos crea una tabla con: las direcciones IP de origen y destino, números de puertos, números de secuencia de los paquetes y otros datos adicionales asociados a la conexión en particular. Gracias a esto, el firewall puede implantar las políticas de seguridad definidas por la empresa con una gran conciencia de la aplicación que se está ejecutando. Así se asegura que los paquetes que no estén asociados a una conexión no pasarán a través del firewall.

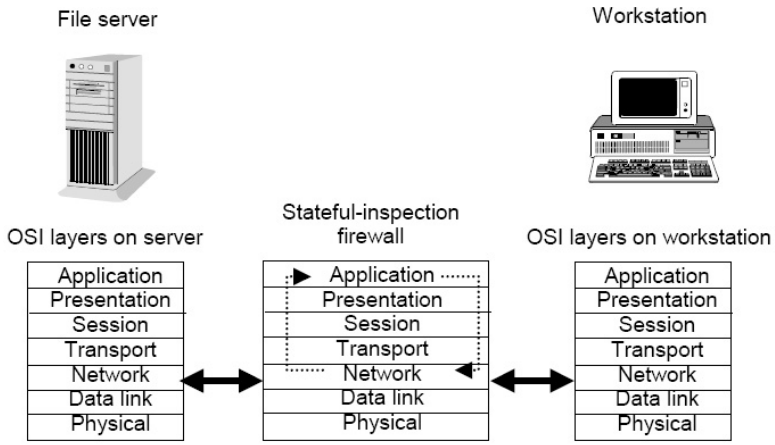


Fig. A.5 Stateful Multi-Layer Inspection

Con respecto a la seguridad que ostenta, no es capaz de evitar los ataques enmascarados más sofisticados a nivel de aplicación, como desbordamientos de búfer o comandos de aplicación ilegales o inseguros. Por ello, la mayoría de expertos en seguridad creen que la arquitectura de cortafuegos basados en pasarelas de aplicación son más seguros que los sistemas basados en filtrado de paquetes, incluso SMLI.

A.1.4. Circuit Level Gateway

Este dispositivo utiliza el mismo sistema de control que la pasarela, aunque en este caso no trabaja a nivel de aplicación sino que lo hace en sesión (como se observar en la figura A.6). Su trabajo es hacer de intermediario en las sesiones TCP entre los usuarios autorizados en la red interna y externa.

Durante toda la sesión controla que los valores de SYN y ACK sean coherentes para evitar que algún intruso quiera colarse. Para ello, guarda la información de las sesiones en unas tablas creadas en el momento de la inicialización de la

sesión TCP. Al finalizar la sesión, la tabla correspondiente a la conexión, es eliminada, y cualquier intento externo de continuar es bloqueado.

La ventaja de este sistema es que permite controlar las conexiones por puertos, pero la de gran desventaja de este tipo de sistema es que no verifica el contenido de aplicación de la comunicación. Por lo tanto, pueden colarse amenazas por las capas altas de las sesiones.

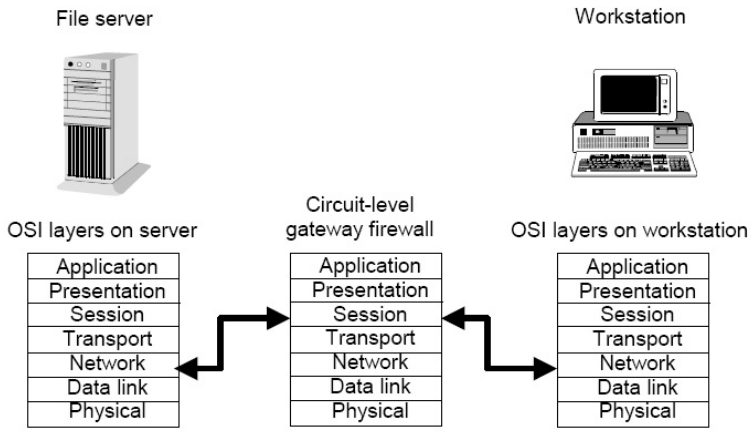


Fig. A.6 Circuit Level Gateway

ANEXO B. LAS AMENAZAS A MPLS VPN

B.1. Las VPNs

Las VPNs son el elemento básico para la interconexión de sedes y proporcionar a los Clientes transferencia de datos privada. Pero como para todos los elementos, existen posibles amenazas de la red. Las más probables pueden llegar: desde el interior o desde un ataque DoS.

B.1.1. Posibles intrusos

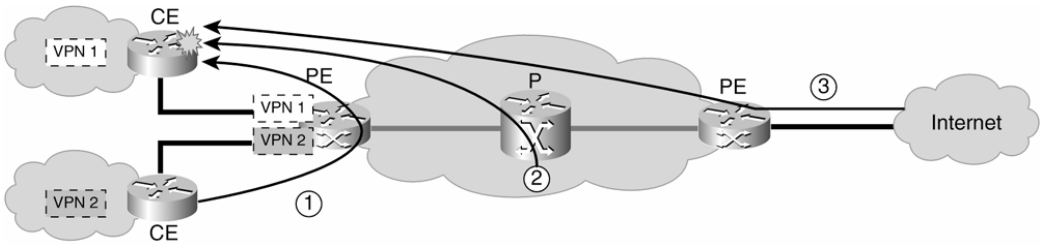


Fig. B.1 Posibles puntos de intrusión

En la figura B.1 se muestran dos VPNs con una sola red base. Una de las VPNs dispone de una conexión a Internet. Esta, precisamente, sirve para mostrar los 3 grandes focos de posibles amenazas:

- Amenazas de otras VPNs (1): Las interfaces externas de las PEs son visibles, y por ello pueden ser un centro de posibles ataques. Estos ataques, posiblemente de DoS, podrían afectar al servicio del resto de VPNs en el mismo PE. De todas maneras, la separación de VPNs ayuda preservar la seguridad entre VPNs con lo que los posibles ataques a una VPN no deberían afectar ni al resto de VPNs ni al core.

- Amenazas del propio core (2): En caso de que se desconfiguraran las rutas, podría provocar que VPNs que no deberían estar unidas lo estuvieran. Con lo que usuarios externos podrían introducirse en la red del cliente. Este tipo de desconfiguraciones pueden ser fortuitas o provocadas.

- Amenazas de Internet (3): Es muy sencillo considerar Internet como una gran amenaza, teniendo en cuenta la gran cantidad de virus y troyanos que circulan por ella. El servicio de Internet pude fluir tanto a todos los miembros de a sede a través de un hub-and-spoke, para centralizar y tener un mejor de la seguridad, como utilizar firewall y detectores de intrusos sin centralizar la conexión.

De todas maneras, siempre se recomienda que los clientes instalen un firewall para evitar posibles amenazas externas, y filtrar aquellas rutas que no pertenezcan a su propia VPN.

B.1.2. DoS

El ataque de negación de servicios es la amenaza más potente a la que se enfrenta cualquier elemento de red. Comparado con el caso anterior, en que una buena gestión de la entrada de paquetes (a través de un firewall, por ejemplo) puede controlar la amenaza, en DoS se deben tomar más medidas.

Los puntos por donde se puede colar este tipo de amenaza, se extiende a toda la red (tal y como muestra la figura B.2). Tanto pueden originarse en el core (PEs y Ps), como por redes externas como Internet o extranets.

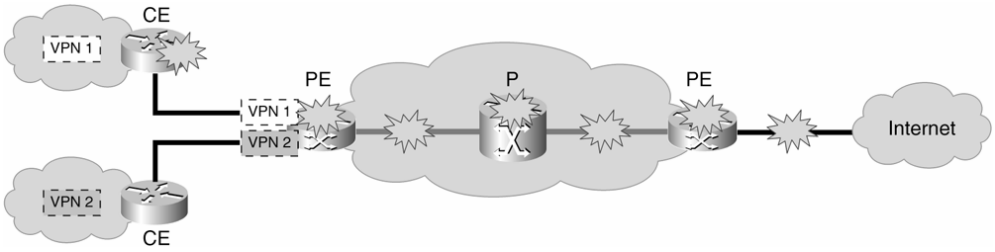


Fig. B.2 Posibles puntos de ataque DoS

Por otro lado, y como se comentó en el caso interior, el ataque a una PE con DoS puede llegar a afectar al resto de VPNs de la PE. De forma que sus recursos se reduzcan, aunque el ataque no pasaría a las VPNs ni a sus sedes.

B.2. La extranet

Por extranet se puede entender:

- Intranet y extranet integrados: El propósito de este tipo de conexiones es unir diversas VPNs entre sí.

- Central de servicios: En este caso la idea es que diversas VPNs tengan una sede, un punto en común.

Des de el punto de vista de seguridad, este tipo de uniones padecen el mismo tipo de amenazas que para un VPN sola. Ya que, a nivel lógico, para un PE estas VPN y/o sedes VPN también son una sola VPN.
De igual manera, la inclusión de un firewall ayuda a mantener al separación requerida entre las redes privadas de cada sede y las del resto de sedes añadidas.

B.3. El Core

Vimos en ATM que su backbone era una fuente de posibles ataques, y como en todas las redes, MPLS VPN también tiene su repertorio. Las diferentes maneras de presentar el core: única o múltiple (Inter-AS, CsC); contienen más o menos las mismas precauciones.

Por otra parte, existe también una red llamada NOC (*Network Operations Center*) que gestiona todas las operaciones entre redes. Esta red vinculada a nivel lógico con la red, también debe ser comentada en este anexo por su implicación con las redes externas como Internet y extranets.

B.3.1. Core único

Como bien dice el encabezamiento, el core único (o core monolítico) lo forma una sola red base. Este tipo de infraestructura puede padecer las siguientes amenazas:

- Intrusiones desde el exterior: La única manera de poder protegerse de este tipo de ataques, es creando un buen control de las operaciones internas. Es evidente, observando las diferentes figuras, que el primer punto por donde se pueden producir los ataques es por una PE. De cualquier manera, ni las VPNs ni Internet no pueden acceder al core. La única comunicación que existe es entre los PEs y los CEs. Aunque estos pueden filtrar el tráfico únicamente a las interfaces y los puertos permitidos.

- DoS desde el exterior: Cualquier parte del core MPLS es potencialmente vulnerable a un ataque de este tipo desde Internet o una VPN. Sin embargo, la imposibilidad del acceso desde el exterior al core, hace que este tipo de ataque se rebaje a una inundación al PE y la VPN afectada. La única manera de asegurar el core, es haciendo que los servicios y requerimientos de QoS se cumplan (al menos los mínimos) tanto en los PEs como el en resto del core, a pesar de padecer un ataque DoS.

- Internas, como la desconfiguración de rutas: La desconfiguración de las rutas, pueden causar serios problemas entre VPNs. La asociación de VPNs que no debieran estar unidas, podría hacer que los virus, troyanos, gusanos y otras amenazas existentes en una red descuidada, pasaran también a otro Cliente. Por eso se recomienda a los Clientes que sitúen firewalls en las entradas a sus redes. Por otro lado, los operadores instalan en sus redes controles que vigilan los movimientos de los equipos, y descubrir usos indebidos de los sistemas.

B.3.2. Inter-AS

Si en el caso anterior se trataba de una sola red *core*, en este pasamos a situar múltiples redes de servicios como se observa en la figura B.3.

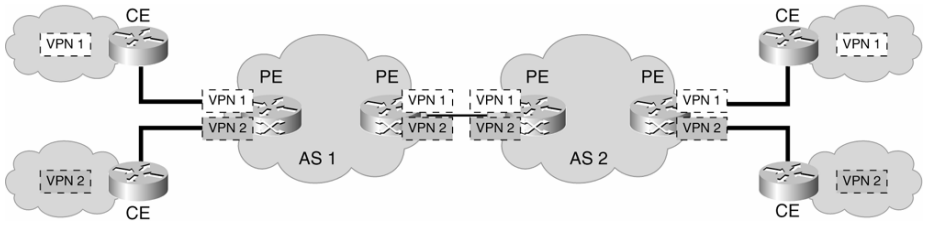


Fig. B.3 Arquitectura de Inter-AS

En este tipo de uniones se siguen padeciendo las mismas amenazas que en el caso de una red única, aunque añadiendo las posibles amenazas procedentes de ASs (*Autonomous System*) vecinos. A nivel de VPN, el riesgo que pueden correr aquellas VPNs que atraviesan varios AS es mayor que si sólo atravesaran uno. Aún así, las VPNs no saben distinguir si han cruzado 1 o varios ASs.

En el RFC 2547bis ("BGP/MPLS VPNs") se describen tres posibles modelos (llamados A, B y C). A nivel técnico, el modelo A es mucho más restrictivo y no hace aumentar los riesgos significativamente. En cambio, los modelos B y C, permiten más interacción entre los ASs lo cual incrementa el riesgo de intrusiones y ataques DoS entre ASs.

Dependiendo del modelo, se pueden considerar las siguientes amenazas:

- Para cada VPN, cada AS puede introducir nuevas sedes conectadas a la VPN. Esto aumenta el riesgo de amenaza por ataque DoS o intrusión
- El enrutado entre ASs supone un gran riesgo para los PEs, ya que pueden padecer ataques de ASs vecinos
- En los modelos B y C cada AS puede enviar tráfico a través de una VPN de otra AS, sea o no compartida. Este tipo de situaciones puede ser utilizada para ataques DoS o intrusiones

B.3.3. Carrier's Carrier (CsC)

Este modelo consigue una asociación jerárquica entre ASs. En la figura B.4, el *AS2* es un "*Customer Carrier*", el cual utiliza al *AS1* (*Provider Carrier*) para transportar la información a las sedes de las VPNs del otro extremo. Para *AS1*, la información sobre los distintos Clientes no le importa. En este caso el *AS1* solamente transporta los paquetes enviados a través de la interfaz común (CE-PE).

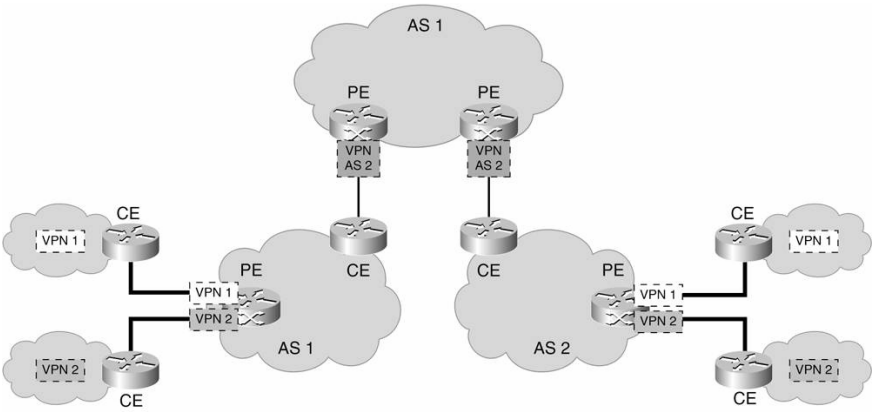


Fig. B.4 Arquitectura de CsC

Para poder hacer el transporte de los paquetes, el *AS1* añade una etiqueta a la etiqueta que añade *AS2* en el PE de su red. Tal y como ocurre en el caso del etiquetaje único, para el proveedor (*AS1*), sólo le interesa su etiqueta. De la misma manera que para el *AS2*, la etiqueta de *AS1* no tendría ningún sentido.

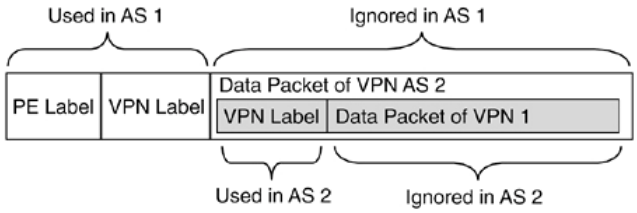


Fig. B.5 Etiquetaje en *AS1*

La utilización de este tipo de etiquetaje provoca que no se posible atacar la red *AS1* desde *AS2*, ya que las direcciones permanecen ocultas como para el caso de una simple AS. Así pues, cualquier ataque contra el CsC no supondría una amenaza. El ataque se mantendría dentro del dominio de *AS2* o dentro de su VPN.

B.3.4. Network Operations Center (NOC)

Estas redes de control están lógicamente separadas de la red core. Pueden existir más de una pero permanecen independientes entre sí.

Sus operaciones, abarcan todas las redes externas que puede tratarse en una backbone: Internet, Intranet, y otras redes (como se ilustra en la figura B.6). Las amenazas pueden llegar de cualquiera de las redes. Las intrusiones producidas por estas redes pueden atacar las redes de gestión o sistemas como servidores FTP (*File Transfer Protocol*) y TFTP (*Trivial File Transfer Protocol*), servidores AAA (*Authentication, Authorization, and Accounting*), etc.

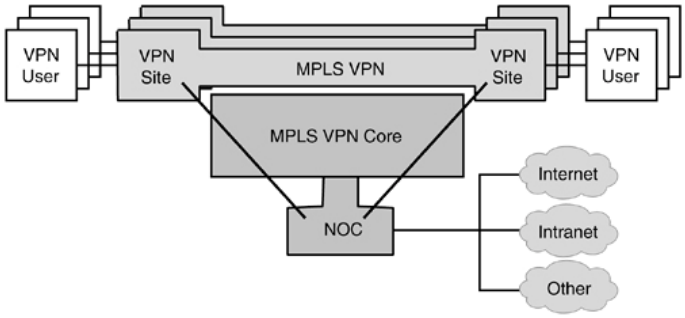


Fig. B.6 Esquema de NOC

Los posibles ataques a este tipo de redes pueden producir grandes efectos en la gestión y el mantenimiento de las redes. Por esta razón, los proveedores procuran proteger sus redes de operaciones a través de filtrajes y listas de acceso.

B.4. Internet

Internet es una red insegura para todos sus usuarios, y puede suponer un problema para los proveedores de servicios. Todos los usuarios de esta red, tal y como se recomienda a los Clientes de los proveedores de servicios, tendrían que asegurar sus redes. Por ejemplo, la utilización de simples firewalls apaciguaría un poco todas las amenazas existentes en la red.

Aún así, los proveedores de servicios deben aplicar grandes medidas de seguridad para evitar los posibles ataques spoofing y DoS. Una manera sería siguiendo las recomendaciones del RFC 2827, donde se explica la incorporación de filtrado de paquetes en los routers de entrada.

B.5. Zonas de confianza – zonas inseguras

Se entiende por zonas de confianza, los puntos compartidos por dos redes o VPNs. El uso inseguro de estas zonas, puede facilitar el paso a posibles ataques de las redes vecinas.

A veces no se tiene en cuenta que la zona de confianza esta situada justo en una zona conectada a una red MPLS. Es evidente que este tipo de zonas, y por el compromiso mutuo que debe existir en temas de seguridad entre el proveedor y el cliente, debe protegerse. Algunas de los puntos olvidados son:

- Punto de acceso *wireless* sin control de acceso en una empresa con servicio MPLS VPN.

- Un ataque DoS desde Internet a un servidor web de una red VPN, donde tanto la VPN como el servicio Internet son proporcionados por el mismo core MPLS.

- Un intruso desde una VPN MPLS dentro de otra VPN, atravesando los puntos de la interconexión que se diseñan específicamente para este propósito, por ejemplo Extranets.

- Infecciones por gusanos procedentes de una sede VPNs a otra, de una extranet que las conecta entre sí.

Como en muchos otros casos, las dos últimas situaciones se pueden resolver con la colocación de un firewall. Con la correcta gestión de los filtros, se puede asegurar una buena protección contra amenazas externas, y también las de la propia VPN.

ANEXO C. EVOLUCIÓN DE LA TECNOLOGÍA *BACKBONE*

C.1. Exigencias del mercado

Una de las grandes razones de la situación en auge de las tecnologías de las telecomunicaciones, es el uso exponencial que tubo Internet a finales del siglo pasado. Posiblemente, el primer paso hacia esta aceptación surgió a principios de los ’90 cuando los operadores de servicios de telecomunicaciones empezaban a usar de la tecnología IP para ofrecer servicios de paquetes en detrimento de la tecnología X.25 (de gran aceptación en Europa). Para ello se utilizaba la infraestructura existente pensada para servicios que emplean circuitos como la voz o las líneas punto a punto. Diez años después, las redes IP son vistas como el medio “universal”, dónde poder transportar diversos tipos de tráfico, tales como voz, video y datos. La capacidad de estas redes, continúa creciendo a medida que las aplicaciones de ocio derivadas del acceso de banda ancha generan nuevos para su capacidad.

Entre las tentativas más importantes de integración del transporte del tráfico se encuentra ATM (*Asynchronous Transfer Mode*), desarrollado entre finales de los ’80 e inicio de los ’90. ATM es un estándar con características muy interesantes, entre las cuales:

- Elevada velocidad de conmutación
- Posibilidad de diferenciar la calidad de servicio
- Mecanismos de control y gestión del tráfico muy eficiente

Aunque estas características eran muy del agrado de las operadoras, la realización práctica y su funcionalidad era un impedimento para su utilización en aplicaciones de usuario.

A partir de los primeros años de los ’90, la introducción de nuevas aplicaciones (como por ejemplo el servicio WWW) basadas en un plataforma simple y estandarizada como la arquitectura protocolar TCP/IP bastaba para satisfacer el mercado, pero cambió de hecho la filosofía de uso. Esto provocó inevitablemente la modernización de los fabricantes de dispositivos y de los gestores de red, intentando encontrar la vía de optimización de las redes IP. De hecho, este cambio de filosofía hizo entender a las grandes compañías del sector, que el mundo de las telecomunicaciones dejaba de ser meramente un producto para la investigación, para pasar a ser un producto bajo demanda. Desde ese momento, no eran las empresas del sector las que determinaban el camino a seguir, sino que por primera vez se trabajaba para satisfacer las exigencias del mercado.

C.2. Problemas a resolver

Era clara la falta de concordancia entre las exigencias de un mercado cada vez más exigente y el nivel de las infraestructuras. Por esta razón se veía evidente hacer un estudio de la situación para, a partir de los recursos disponibles, efectuar los cambios convenientes.

Durante los dos próximos puntos se reflejaran aquellos aspectos más importantes, que fueron estudiados con la intención de mejorar las redes del momento.

C.2.1. Situación general

La situación a la que se había llegado no era forzosamente crítica, pero sin duda hizo que las grandes empresas e instituciones del sector se pusieran manos a la obra. Era necesario cambiar nuevamente la *backbone*, ya que el escenario al que estaban habituados hasta aquel momento no era el más adecuado para las exigencias que se presentaban. Los puntos débiles de la red tradicional IP se podrían resumir de la siguiente manera:

- Imposibilidad de diferenciar la calidad de servicio ofrecida: Las redes IP ofrecen una sola clase de servicio, llamada *Best-Effort*, la cual no ofrece ningún tipo de nivel de calidad de servicio (QoS). Esto significa que no garantiza si o cuándo una unidad será entregada al destino, aunque puede que se pierda si no disponen de recursos en las colas.
  Hasta el momento, las aplicaciones que se utilizaban con más éxito (*e-mail* o *WWW*), no necesitaban ningún tipo de calidad de servicio. No era esencial que no se perdieran paquetes durante la conexión. En cambio el mercado empezaba a exigir más. El tráfico en tiempo real (como voz y video) no podía sobrevivir en una red donde no se respetaban: número de paquetes perdidos, retardos máximos *end-to-end*, y variabilidad del retardo (o *jitter*).

- Imposibilidad de automatización del tráfico de red: En las redes IP, el tráfico se encamina según el algoritmo de búsqueda del camino de menor coste, basado en determinadas matrices asociadas a las conexiones (por ejemplo: el número mínimo de saltos, ancho banda máximo, etc.). Estos algoritmos se basan en la visión “topológica” de la red y no sobre el tráfico de los nodos del camino. Esto puede provocar que puntos concretos de la red se vean saturados por un gran flujo de paquetes, con lo que puede provocar saturación y pérdida de paquetes. Por otra parte, otros puntos de la red menos agraciados según el algoritmo, sean escasamente utilizados. Este tipo de situaciones indican una utilización poco óptima de la red.

- Escasa escalabilidad en la oferta de servicios: Servicios como Redes Privadas Virtuales (VPNs) basadas en la plataforma IP, creaban serios problemas de gestión en caso que fueran demandadas conexiones de

millares de clientes-empresas, cada uno de los cuales con diversos centenares de sitios-sedes a interconectar.

Con estos tres puntos claros, a partir de la mitad de los años ’90, se inició un movimiento de impulso para mejorar las redes IP otorgándoles más velocidad, escalabilidad y seguridad.

Viendo las grandes perspectivas de futuro y los tres grandes puntos a mejorar, las grandes empresas se dieron prisa para sacar sus propias propuestas. Años más tarde, la IETF hizo su propuesta de estándar basado en las mismas ideas básicas que sus predecesoras. Llamaron a este estándar, MPLS (Multi-protocol Label Switching).

C.2.2. El *Core*, la base del cambio

Si realmente se quería llegar a una “modernización” de la red IP, y conseguir una arquitectura de red que pudiera englobar todos los tipos de protocolos y aplicaciones existentes, el *Core*, el núcleo de la red IP, debía ser parte del estudio.

Al estudiar el *Core*, para intentar adecuarlo a las nuevas exigencias, se pudo observar un gran problema, pues históricamente las redes de telecomunicaciones se han desplegado de forma que cada servicio, según la tecnología empleada, definía la infraestructura a emplear. Esta aproximación provocó que se crearan redes inflexibles, e incapaces de amoldarse a los nuevos requisitos de servicio. Por ejemplo, las redes de voz, las de circuitos de datos basadas en *Frame Relay/ATM*, las de ámbito metropolitano de alta capacidad basadas en *Gigabit Ethernet* o las redes de paquetes IP basadas en varios tipos de infraestructura.

Esta situación comentada, ocasionó que los operadores de servicios se plantearan la idea de crear redes de nueva generación capaces de acomodar esos servicios que surgían y surgirán. Las características de las cuales pueden ser:

- La demanda creciente de servicios de banda ancha, con apoyo de las administraciones públicas. En este aspecto, el Gobierno Central ha anunciado la reducción progresiva de las cuotas del *adsl* con el aumento progresivo de la velocidad de las conexiones. Esto fomenta que cada vez más, la ciudadanía opte por contratar este tipo de servicios.

- La tendencia hacia el modelo de “*triple play*” (datos de alta velocidad, voz sobre IP (*VoIP*) y televisión sobre IP (*TVoIP*)) incluyendo servicios de ocio (juegos en red, TV bajo demanda). Esta tendencia a la alza, mediatizada por las grandes operadoras de servicios exige un gran ancho de banda y un gran nivel de gestión. Esto requiere una

optimización de las redes centrales, muy por encima de lo requerido hasta el momento.

- La reducción de margen en los servicios tradicionales con la consiguiente reducción de costes de operación de estos servicios. Un ejemplo es la transmisión de voz.

Una red de nueva generación tiene como referentes: la movilidad de las redes inalámbricas, la fiabilidad de la red pública conmutada, el alcance de Internet, la seguridad de las líneas privadas, la capacidad de las redes ópticas, la flexibilidad del *Core* para la integración de servicios de datos, voz y vídeo; así como la eficiencia que conlleva la operación de una infraestructura común y consistente.

La aportación fundamental de estas redes de nueva generación y, en particular, de su núcleo, es la convergencia, que permite que podamos hablar de servicios de datos, de voz y de vídeo como hasta ahora. La convergencia tiene lugar en dos niveles:

- Infraestructura: Es el efecto de consolidar el transporte de datos, voz y vídeo, realizado tradicionalmente sobre distintas redes, sobre un *backbone* común de paquetes.

- Servicio: En este caso, la convergencia significa que al integrar los servicios de datos, voz y vídeo sobre tecnología de paquetes IP, esto permite acceder a las funciones propias de esta tecnología, es decir, calidad de servicio, seguridad (detección de intrusión, cortafuegos gestionados), almacenamiento, video bajo demanda, etc.

Esta convergencia puede otorgar una gran capacidad a la red para transportar y gestionar diferentes tipos de servicios y protocolos. El problema es que para ello, se deben instalar equipos en la red capaces de asegurar-cumplir los requisitos de escalabilidad, disponibilidad y flexibilidad que plantea el *Core* de las redes de nueva generación.

C.3. Punto de partida: IP/ATM

Desde que en los primeros años de los ’90, apareciera el estándar ATM; poco después se optaba por la utilización de paquetes marcados con IP. Estas dos “tecnologías” unidas, han otorgado a las antiguas redes universitarias y empresariales, la opción de expandirse hacia las grandes masas comerciales. Ahora, IP/ATM está dejando paso a otra “tecnología” que desbancará esta para otorgar a las redes mucha más progresión.

Antes de seguir con el presente y el futuro, y siguiendo la línea perseguida hasta el momento, durante los próximos dos puntos se podrán ver unas pocas pinceladas de las características básicas de IP y ATM. Con ello, se podrá al

menos entender las alternativas que surgieron a esta conjunción, a IP/ATM, entre ellas MPLS.

C.3.1. El protocolo IP

El Protocolo Internet (Internet Protocol), o Ipv4 es la parte central del paquete de protocolos de Internet. IP (RFC 791, RFC 1122) es un protocolo de red que ofrece un servicio de envío de paquetes no orientado a conexión. Sobre éste trabajan los protocolos de transporte, siendo el más común de ellos el protocolo TCP. Por ello es habitual encontrarnos con el término TCP/IP en referencia al funcionamiento conjunto de los protocolos.

IP es un protocolo orientado a datagramas que trata cada paquete de manera independiente, de modo que cada paquete deberá contener toda la información necesaria para ser encaminado de manera correcta. No tiene garantías de entrega de paquetes ni garantías de integridad en la información recibida, ya que ni emplea el *checksum* para comprobar el contenido del paquete, ni posee mecanismos de confirmación para determinar si el paquete ha alcanzado su destino.

El protocolo IP junto con protocolos como ARP, RARP o ICMP define el formato del datagrama, direccionamiento, procesamiento de paquetes, routing y mecanismos para mostrar errores en Internet. Tal y como se describe en el RFC 1122, un host que esté ejecutando el protocolo IP, normalmente también admitirá ARP y ICMP.

En la versión 4 de IP, el espacio de direcciones está limitado a 32 bits. Una dirección comienza con un número de red, empleado para el routing, seguido de una dirección local, para la red interna. Bajo estas direcciones, también se sustenta la posibilidad de enviar paquetes-datagramas en modo Multicast (a todos los miembros de un grupo de la red) y Broadcast (a todos los miembros de la red).

Actualmente, a causa de la escasez de direcciones IP, se baraja la alternativa de ampliar la versión 4 de IP. A esta alternativa la llaman IPv6 o IPng (*Next Generation Internet Protocol*). Diseñado por el IETF, esta solución mantiene todas las funciones utilizadas en IPv4, y el resto se quitan o se hacen opcionales. Con todo ello, se intentan solucionar algunos problemas que presenta la versión 4 añadiendo un mayor espacio de direccionamiento (RFC 2373) pasando así de 32 a 128 bits, un sistema de seguridad (RFC 2401 y RFC 2411), una maquinaria de Autoconfiguración (RFC 2462) y una mejor adaptación a los requisitos de movilidad (o *roaming*) (RFC 3024).

C.3.2. La Tecnología ATM

La *Asinchronous Transfer Mode* (ATM) fue definida en un principio por la ITU-T (*ITU Telecommunication Standardization Sector*) en 1988, una organización compuesta principalmente por los operadores de redes públicas. Posteriormente se

fundó el ATM Forum (en 1991), que aceleró el desarrollo de los estándares relacionados con esta tecnología. El ATM forum está compuesto por compañías que trabajan sobre redes privadas y comunicaciones de datos.

El Modo de Transferencia Asíncrono (*Asynchronous Transfer Mode*) ó ATM es una tecnología de conmutación orientada a conexión y basada en el envío de celdas. Estas celdas tienen la peculiaridad de que son de tamaño fijo (53 bytes). Este valor, muy pequeño respecto al tamaño máximo de un datagrama IP (65.535 bytes), proporciona a los paquetes ligereza a la hora de ser encaminados y la posibilidad de que los conmutadores "entrelacen" diversos flujos a la vez.

Por otra parte, ATM es asíncrono, esto significa que las celdas que contienen información de usuario no necesitan ser enviadas de manera periódica. Esta característica, junto con las ventajas de las celdas, son las que hacen posible transportar tanto tráfico orientado a circuitos como orientado a paquetes, con una transparencia completa para las aplicaciones. ATM ha sido diseñado para dar grandes anchos de banda bajo demanda. De esta manera, ATM fue el primer de los grandes pasos para otorgar QoS a las redes del momento. Entre otras características novedosas, cabe destacar que cuando un usuario no necesitaba acceder a una conexión de red, el ancho de banda de esta conexión se hace accesible para otra conexión que la necesite. Así la red puede obtener un porcentaje de utilización mucho más elevada que en casos anteriores.

C.3.3. IP y ATM: Convivencia obligatoria

A finales del siglo pasado el gran auge de un Internet inseguro y sin calidad de servicio hacía presagiar un cambio obligatorio. IP se había diseñado para proporcionar funciones de interconexión de redes capaces de funcionar sobre una gran variedad de tecnologías, pero le restaban características multimedia.

Por otro lado, ATM se diseñó para proporcionar calidad de servio (QoS) extremo a extremo soportando un gran rango de servios. En parte, por estas razones, ATM tuvo una gran acogida ya que aportaba ventajas importantes sobre las tecnologías existentes para redes de área local y redes de área extensa, incluyendo la tan preciada escalabilidad y la demandada garantía de QoS. Sin embargo, todas estas ventajas que introducía ATM en el mercado se veían empañadas por su complejidad. Esto venía dado por la necesidad de una estructura de protocolo muy compleja para conseguir un alto rendimiento de los conmutadores ATM y el desarrollo de estas redes.

Evidentemente se podría pensar que esas complejidades tecnológicas se podrían salvar algún día. Pero lo que hacía necesaria la convivencia entre IP y ATM, es que la primera tenía prácticamente todo el mercado de software acogido a su mano y, ATM no podía competir con eso por muchas cosas buenas que aportara.

C.3.4. Arquitecturas de encaminamiento IP

El crecimiento tan elevado de Internet, no hacia más que saturar las infraestructuras existentes en las redes troncales. Este es un problema que empezó en aquellos años del siglo pasado y que aún hoy sigue dando que hablar.

Para mantener el rendimiento de esas infraestructuras y evitar el colapso por congestión, los proveedores de servicios actualizaban constantemente sus enlaces troncales, normalmente con tecnología ATM. Estas actualizaciones en los enlaces de transmisión también acarreaban la actualización de los dispositivos de encaminamiento y los conmutadores, para poder seguir operando a la misma velocidad. Inevitablemente se tuvieron que hacer cambios en la arquitectura de los dispositivos de encaminamiento para alcanzar un mayor rendimiento. Por ello se desarrollaron una serie de soluciones de encaminamiento IP resumidas en la siguiente figura C.1.

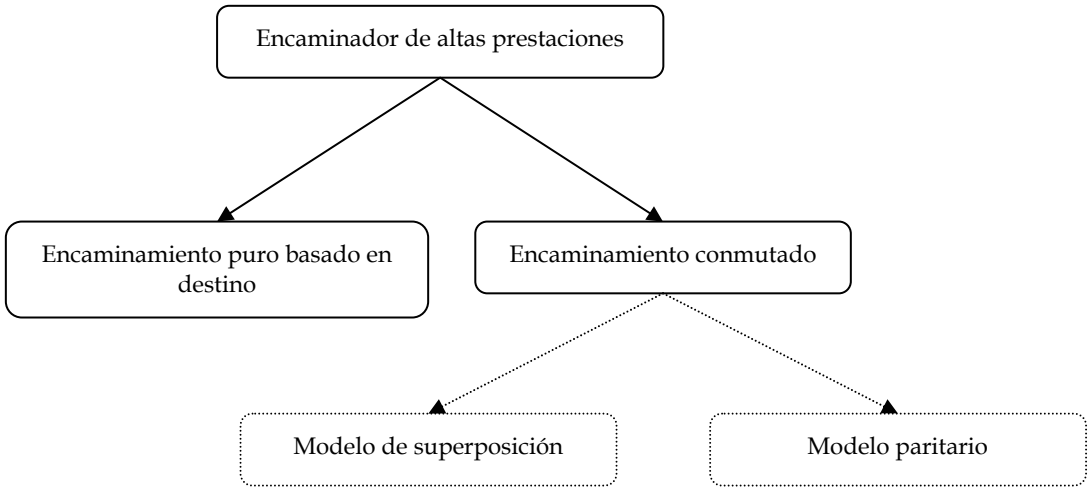


Fig. C.1: Taxonomía de encaminamiento IP

Como primera propuesta, el encaminamiento puro basado en destino esta completamente basado en la arquitectura de dispositivos de encaminamiento convencional, pero resuelve el cuello de botella en los dispositivos de encaminamiento tradicionales modificando la arquitectura de la backbone. La gran mejora, es la posibilidad de poder efectuar envíos simultáneos de paquetes.

Por otro lado, el encaminamiento conmutado simplifica el proceso de búsqueda en la tabla utilizando etiquetas cortas de tamaño fijo, en lugar de los prefijos IP grandes de longitud variable. Una forma típica de simplificar este proceso es ejecutar IP sobre ATM, que utiliza los VPI (*Virtual Patch ID*) y VCI (*Virtual Circuit ID*); tratados en el *Anexo D*. Por ejemplo, la búsqueda con etiqueta en ATM utiliza simplemente el valor VPI/VCI de entrada, el puerto de salida y otra información relevante.

Como se puede observar en la figura C.1, el encaminamiento conmutado se puede clasificar en:

- Modelo de superposición (*overlay*): En este caso, los conmutadores ATM no son conscientes de las direcciones IP y de los protocolos de encaminamiento IP. Este modelo superpone una red IP encima de una red ATM, creando dos infraestructuras de red con dos esquemas de direccionamiento y dos protocolos de encaminamiento. Cada sistema final utiliza la dirección IP y la dirección ATM, que no están acopladas. De esta forma se necesita un protocolo de resolución de direcciones para pasar de una dirección a otra. Una de las ventajas es que la infraestructura ATM se puede desarrollar de forma independiente a la infraestructura IP. Ejemplos de este modelo pueden ser: “IP sobre ATM clásico” (*Anexo D*) y MPLS.

- Modelo paritario (*peer-to-peer)*: Utiliza las direcciones IP existentes (o las direcciones ATM derivadas algorítmicamente) para identificar los sistemas finales y utiliza los protocolos de encaminamiento IP para establecer conexiones ATM. Una de las ventajas de este modelo es que no necesita un protocolo de resolución de direcciones para interconectar los diferentes puntos de la red. Un nodo tiene normalmente un conmutador ATM integrado y una función de encaminamiento IP, de forma que el nodo se puede ver como una pareja de otros dispositivos de encaminamiento. El *peer-to-peer* mantiene una sola infraestructura de red. El mejor ejemplo de este modelo es MPLS (*Anexo E*).

De estos dos tipos de modelos, IP sobre ATM fue el que tuvo más aceptación. Sólo hacía falta actualizar las infraestructuras (dispositivos de encaminamiento, conmutadores,…) para poderlos adaptar al modo de superposición. Esas actualizaciones se hicieron extensibles a todos aquellos problemas que ATM comportaba en infraestructuras y redes más concretas. Por ello, el ATM Forum desarrolló propuestas como LANE (*LAN Emulation*), NHRP (*Next-Hop Resolution Protocol*) o MPOA (*Multiprotocol over ATM*). Todas ellas ayudaron a unificar aún más las diferentes redes y conseguir una infraestructura de red global, que las concentrara a todas.

Incluso, con estas “actualizaciones” y el gran empeño, por parte del ATM Forum por situar el IP/ATM como firme modelo de futuro, los altos costes para actualizar la pila de protocolos de las LAN, el bajo nivel de utilización de la red y la complejidad de las aplicaciones, facilitaron el paso a MPLS .

ANEXO D. IP SOBRE ATM. EL PASADO

En este anexo se introducirán las propuestas de ATM con IP que se desarrollaron. De esta manera, se expondrán las razones por las que optó por buscar otra tecnología que pudiera abarcar todas las necesidades del mercado. Este anexo es el complemento ideal del capítulo 3, para observar claramente la evolución, el antes y el después de esta tecnología que es la base de las redes actuales.

D.1. Del modelo *Overlay* a GMPLS

Desde el fuerte impulso para mejorar las redes IP, buscando otorgarles más velocidad, escalabilidad y seguridad, han existido dos grandes modelos de integración.

Las grandes operadoras optaron por utilizar la mejor tecnología de red que había en aquel momento, ATM. La integración de IP/ATM, en su versión del modelo de superposición u *overlay*, fue el primer paso hacia la incorporación en las redes backbone de la tecnología IP. Pero, las grandes carencias y dificultades de su implementación, obligaron a buscar otra alternativa.

Por esta razón, se optó por el modelo paritario o *peer-to-peer,* que permitió eliminar algunos de los defectos que presentaba el modelo *overlay*, aunque no algunos problemas intrínsecos del transporte de IP sobre ATM. Los principales constructores mundiales desarrollaron, a partir de la mitad de los años ’90, interesantes soluciones propietarias basadas en el concepto de modelo *peer-to-peer*. El gran problema era la falta de interoperabilidad entre ellas, provocada por la falta de afinidad entre las diferentes compañías y sus soluciones propietarias.

Aún así, la validez del modelo *peer-to-peer* fue rápidamente reconocida por la comunidad IP. En particular por Cisco, en el año 1997, anunciando la intención de estandarizar su tecnología propietaria *Tag Switching* implementada, por aquel entonces, en sus routers.

El objetivo era eliminar los inconvenientes del modelo paritario y definir un nuevo estándar basado en gran parte en la tecnología *Tag Switching*. A principios del 1997 se creó en el IETF, un grupo de trabajo con el objetivo de integrar las distintas soluciones propietarias que se habían presentado hasta entonces:

- *Cell Switching Router* (CSR), desarrollada por Toshiba
- *IP Switching*, de Ipsilon
- *Aggregate Route-based IP Switching* (ARIS), presentada por IBM, y
- Tag Switching, de Cisco

El objetivo era desarrollar un estándar que pudiera ser empleado sobre cualquier tecnología de transporte. En abril de ese mismo año decidieron llamarlo MPLS.

Actualmente MPLS es un de las realidades más importantes de las redes modernas IP. Son muchos los gestores que lo han implementado en sus redes y ofrecen servicios basados en este nuevo paradigma.

D.2. Modelos de convergencia para IP - ATM

Las soluciones desarrolladas para ayudar al empleo de las técnicas IP sobre la solución ATM, se han implementado en dos modelos, del cual el segundo puede considerarse una evolución del primero:

- Modelo de superposición o *overlay*
- Modelo paritario/integrado o *peer-to-peer*

El modelo *overlay* se implementa a través de la propuesta de establecer niveles separados y superpuestos, en los que los protocolos de encaminamiento existentes a nivel de IP y ATM trabajan separados e independientes uno del otro. En el modelo *overlay* existe una neta separación entre la red IP y la red ATM, dónde ATM une routers IP.

Por su parte, el modelo *peer*, se contrapone al modelo *overlay* ya que propone eliminar todos aquellos aspectos sobrantes entre las dos tecnologías. En aspectos como el modo de envío de la información y de unificar las estrategias de enrutado, eliminando de la red el enrutado ATM.

Se hicieron distintas propuestas para llegar a una solución global. Los distintos organismos intentaron, a partir de los dos modeles dados, idear propuestas el máximo de próximas al planteamiento ideal.
Tal y como se expresa en la figura D.1 (extraída del libro "*Integrated Broadband Networks*"), ATM Forum e IETF presentaron sus propuestas por separado. Entre ellas destacan el CLIP (Classical IP over ATM) que es el estandarte del modelo *overlay* por su parte, en el modelo paritario (o integrated, como se expresa en el libro) tiene como gran baza el MPLS over ATM, antecesor al actual MPLS over VPN.

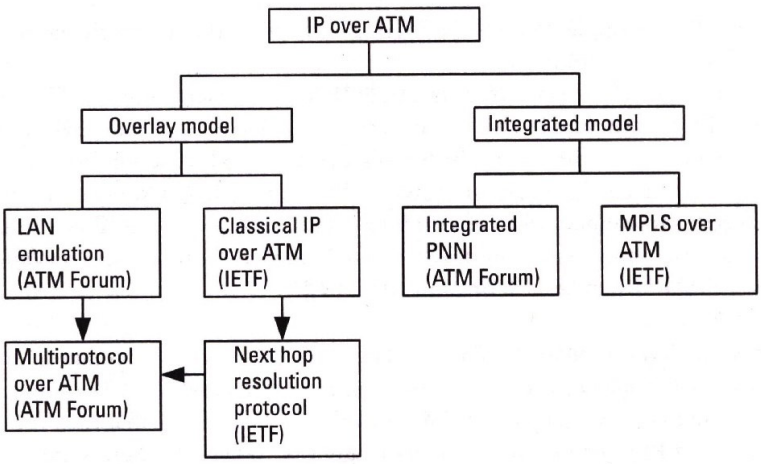


Fig. 2.1: Taxonomía de los modelos IPoA

D.2.1. El modelo *overlay*

El modelo overlay fue adoptado por las grandes redes IP a partir de la mitad de los años ’90, cuando iniciaron el proceso de búsqueda de soluciones que pudieran satisfacer el creciente volumen de tráfico de Internet.

Hacia la mitad de los años ’90 los principales gestores de redes estuvieron prácticamente obligados a cambiar sus redes para poder soportar velocidades mayores a 155 Mbps. Muchos gestores hasta entonces, habían realizado redes utilizando routers con interfaz ATM a 155 Mbps y switchs ATM con interfaz a 155 Mbps en la *backbone* de la red ATM, y tuvieron que dar paso a cambios en la infraestructura para alcanzar los 622 Mbps.

Entrando en materia, este modelo utiliza el modelo IP clásico sobre ATM especificado en el RFC 1483. In particular utiliza la versión con Conexiones Virtuales Permanentes (PVC, *Permanent Virtual Connection*). Estas conexiones se establecen de manera que “lógicamente” puede observarse una topología de red totalmente mallada. Sin embargo, los routers no conocen la topología física de la red ATM, pero sí que son conscientes de la red PVC establecida entre ellos y sus homónimos. Los routers, por lo tanto, quedan emparejados entre ellos como simples conexiones punto-a-punto.

Sobre cada una de las conexiones PVC actúa un protocolo de enrutado que los routers pueden establecer con sus homónimos, e intercambiarse las informaciones de enrutado. Típicamente todas las PVCs ATM están configuradas con categorías de servicio del tipo UBR (*Unspecified Bit Rate*) o ABR (*Available Bit Rate*).

En lo que respecta al encaminamiento de los paquetes IP, se consigue introduciendo en las clásicas tablas de enrutado IP presentes en cada uno de los routers, la correspondencia entre el Next-Hop y el identificador (local) VPI/VCI del PVC ATM de conexión entre los router origen y destino del paquete.

Y el transporte de los paquetes en celdas ATM se produce utilizando los servicios de adaptación AAL5 (ATM Adaptation Layer) de ATM.

D.2.1.1. Elección de red completamente mallada

Como se ha hecho referencia anteriormente, en este tipo de modelo es utilizada una malla completa (lógicamente hablando). Esto significa que si tuviéramos una red IP con N routers, la red necesitaría configurar *N(N-1)/2* PVC. Esto comporta un elevado número de enlaces del protocolo de enrutamiento IP, que puede llevar a un "estrés" del protocolo llegando incluso a dejar fuera de servicio muchos PVCs, cosa que podría fácilmente producirse, por ejemplo, con la desconexión de un enlace físico y/o nodo de la red ATM (problema del *N-squared*).

En una opción menos agresiva, utilizando por ejemplo una topología de red no-completamente mallada, el paquete IP debe ser reensamblado en cada uno de los routers que atraviesa, para poder permitir el análisis del direccionamiento IP. No hay que olvidar que los paquetes, por pequeños que sean, se particionan en celdas de 53 bytes (incluida su propia cabecera). Esto significa que sobre cargas grandes de la red si los routers no están bien dimensionados, el comportamiento de la red se degrada. Esto explica, en parte, por qué se utiliza la opción de la topología completamente mallada, que aunque mucho más costosa (sobretodo a lo que gestión se refiere), en ella las celdas no deben hacer un recorrido tan escalonado en la red, "únicamente", encaminarse a través de la PVC.

D.2.1.2. Ventajas e inconvenientes

Dejando de banda la arquitectura de la red, las ventajas principales que ofrecía este modelo se podrían resumir en 3 puntos:

- la flexibilidad en las asignaciones de las bandas; con los PVC ATM es posible configurar conexiones de banda arbitraria (también asimétrica si es necesario)
- la posibilidad de aprovechar las funcionalidades ofrecidas por ATM para diferenciar los flujos de tráfico y por lo tanto ofrecer diferentes niveles de QoS
- la posibilidad de gestionar el tráfico de la red, para hacer frente en modo más adecuado a las situaciones de congestión

Como puede observarse, en la simbiosis de las dos tecnologías la que sale más beneficiada es el estándar IP. Los tres puntos señalados arriba, son sin duda características de ATM que a razón de esta expansión conjunta, ayudó a IP a mejorar ciertos puntos olvidados o poco trabajados.

Hoy en día estas características descritas, son como "el pan de cada día". A nadie en este tipo de entornos le extraña hablar de Calidad de Servicio (QoS),

o de gestión de congestión. Sin duda este modelo ayudó a que a día de hoy se planteen nuevos retos, aunque sin olvidar los anteriormente mencionados.

Por otra banda, y a pesar de los avances que consolidó este modelo, hubo una serie de características que pesaron más, y que hicieron que poco a poco se abandonara la práctica del *overlay*. Entre ellas podemos destacar:

- Requiere la gestión de dos redes diferentes: una infraestructura ATM y una red IP lógica sobrepuesta, con todo lo que esto comporta en términos de déficit de gestión
- La limitada escalabilidad de las interfaces SAR ATM (Segmentation And Reassembly ATM), provocado en parte, porque sólo alcanzan hoy en día los 622 Mbps. Aún así, existen interfaces ATM SAR a 2'5-10 Gbps pero podrían no estar nunca disponibles comercialmente a causa del coste y de la complejidad de implementaciones de las funciones SAR a velocidades así

D.2.2. IP sobre ATM clásico

El máximo exponente del modelo *overlay* es IP sobre ATM clásico, más conocido como CLIP (classical IP over ATM). Es una especificación de la IETF expuesta en el RFC 2255, donde IP trata ATM como otra subred a la que se conectan las computadoras y los dispositivos de encaminamiento. En el modelo CLIP las múltiples subredes IP se superponen normalmente encima de una red ATM. La parte de una red ATM que pertenece a la misma subred IP, se llama subred IP lógica (LIS, *Logica IP Subnetwork*). Todos los miembros (sistemas finales IP) en la misma LIS deben utilizar el mismo prefijo de red IP (es decir, los mismos números de red y los mismos números de subred). En este entorno, dos miembros en la misma LIS se comunican directamente a través de una conexión de canal lógico ATM (VCC).
Cada LIS funciona y se comunica independientemente de otros LIS en la misma red ATM. La comunicación con dispositivos fuera de la LIS se debe hacer a través de un dispositivo de encaminamiento IP que esté conectado a la LIS. Por lo tanto, miembros que pertenecen a LIS diferentes se comunican a través de dispositivos de encaminamiento.

D.2.2.1. Resolución de direcciones

Supongamos que en una red modelo CLIP, existen dos ordenadores llamados O y D. Existen dos casos generales de envío de paquetes: en que los dos ordenadores o dispositivos estén situados en la misma LIS, y el caso en que formen parte de subredes diversas.

La primera vez que uno de los ordenadores (digamos O) quiere enviar un paquete a otro ordenador (D) utilizando CLIP, este sólo conoce la dirección IP de D. Para establecer un VCC, S necesita la dirección ATM de D.

En el primer caso dado, la manera de conseguirlo es mediante la implementación de un protocolo de resolución de direcciones ATM (ATM ARP) que actúa en cada LIS. En cada ordenador se configura la dirección ATM del servidor ATM ARP. Cuando se enciende el ordenador, registra sus direcciones IP y ATM en el servidor de la LIS a la que pertenece. Cuando un ordenador quiere resolver la dirección ATM de otro ordenador a partir de la dirección IP, pregunta al servidor por esa dirección. Después de que el ordenador reciba la respuesta ATM ARP del servidor, ya puede establecer un VCC con el ordenador destino y enviar paquetes por ese VCC. Este proceso supone la fragmentación del paquete IP en celdas ATM en el ordenador origen y reensamblado del paquete en el ordenador destino.

En el segundo de los casos, el ordenador origen establece un VCC con el dispositivo de encaminamiento conectado en la misma LIS. Este dispositivo examina el paquete IP, determina el dispositivo de encaminamiento del siguiente salto, establece un VCC y envía el paquete. El proceso continúa hasta que ese alcanza el dispositivo de encaminamiento de la LIS del destino y se entrega el paquete a la computadora destino.

D.2.2.2. Ventajas e Inconvenientes

La principal ventaja que aporta es su compatibilidad total con IP estándar, permitiendo a la gran mayoría de protocolos y aplicaciones que se encuentran por encima de éste ejecutarse de manera transparente sobre ATM, aprovechando el gran ancho de banda de ATM. Otra ventaja que aporta es la facilidad de integrar servicios basados en IP con servicios basados en ATM. (por ejemplo, servicios de voz).

El principal problema de esta solución es que no puede alcanzar garantías de QoS de ATM debido a los siguientes motivos:

- Las conexiones ATM directas solo se pueden establecer dentro de un LIS, pero no a lo largo de los extremos. Debido que la resolución de direcciones está limitada a un solo LIS, el tráfico IP entre nodos en diferentes LIS, siempre circulará el dispositivo de encaminamiento, que sólo puede ofrecer *Best Effort* con garantías de QoS.

- Todos los flujos de datos IP entre dos ordenadores comparten el ancho de banda de un solo VCC. De modo que resulta imposible a una aplicación individual conseguir una garantía de QoS para su flujo de datos concreto.

Otro problema de IP clásico sobre ATM es la imposibilidad de realizar *multicast* (ni *unicast*). Además no existe un camino por defecto para enviar datagramas IP antes de que se establezca una conexión, provocando un retraso alto al circular el primer datagrama. Aunque esta solución no permite aprovechar muchos de los equipos LAN clásicos, ofrece un tamaño mayor, y más apropiado de MTU.

Otra de las desventajas, es que introduce un elevado espectro de banda transitiva (cell tax), causada por la necesidad de segmentar los paquetes IP (encapsuladas en la trama AAL5) en celdas ATM. Este espectro es mucho más elevado cuanto más pequeño es el paquete IP a transportar.

La limitación más seria, es el "estrés" del protocolo de enrutado IP. Esto es causado por el elevado flujo de comunicación que debe ser mantenido desde un router y de la complejidad de la utilización de los algoritmos de búsqueda del camino mínimo sobre una topología con un gran número de conexiones.
Como demostración de esta limitación, podemos entrar en el caso de una red completamente mallada. Teniendo como referencia N, como el número de routers de la red, N^4 sería el número de mensajes a intercambiar para reconfigurar las tablas de enrutado.

La solución a este problema es reducir de alguna manera el número de mensajes. Este objetivo es la motivación principal que ha llevado a la idea de un nuevo modelo de integración IP/ATM, el modelo *peer* o paritario.

D.2.3. El modelo paritario

La idea principal del modelo paritario es la reducción del número de mensajes que el protocolo de enrutado debe enviar. Para conseguir este objetivo, la idea es hacer que los switchs ATM se conviertan, desde el punto de vista de encaminamiento, en routers IP.
Esto comporta que la red resultante sea una simple red IP donde los paquetes vienen transportados bajo la forma de celdas ATM sobre conexiones virtuales, que siguen un recorrido que es determinado por un protocolo de enrutado IP (por ejemplo RIP, OSPF, IS-IS).

La realización práctica de esta idea requiere dos requisitos fundamentales:

- introducir la inteligencia de enrutado IP en los switchs ATM, o sea, construir máquinas híbridas (switch IP+ATM) con inteligencia IP y modalidad de comunicación ATM.

- definir un nuevo protocolo para asociar las etiquetas (campos VPI/VCI) de las celdas ATM al recorrido determinado por el protocolo de enrutado IP.

Todas las grandes empresas tienen máquinas y software para satisfacer estas dos grandes demandas, pero sin embargo, siguiendo sus propias ideas de diseño sin una guía estándar.
En 1996/97 eran diversos los constructores que proponían sus propias soluciones propietarias para la integración de IP y ATM según la lógica del modelo *peer*:

- Toshiba: *Cell Switch Router* (CSR)
- Ipsilon Networks: *IP Switching*

- Cisco: *Tag Switching*
- IBM: *Aggregate Route-Based IP Switching* (ARIS)
- Telecom Finland: *Switching IP Through ATM* (SITA)
- Cascade: *IP Navigator*
- NEC: *IP Switching Over Fast ATM Cell TranspOrt* (IPSOFACTO)

Estas soluciones, como suele pasar con todas las propuestas privadas, tienen la gran desventaja de que no son interpolables. Así y todo hay un gran número de características comunes entre todas ellas.
La gran aproximación ha estado adoptar el software del control de un router IP (esencialmente el protocolo de enrutado IP) e integrarlo con el hardware de un switch ATM. En cada uno de los switch IP+ATM se ejecuta un protocolo de enrutado IP (RIP, OSPF, IS-IS, etc.); esto comporta una serie de beneficios, entre los cuales los más importantes son:

- Eliminación del problema de la escalabilidad N-squared
- Reducción del estrés del protocolo de enrutado debido a la notable disminución del número de conexiones que cada uno de los routers debe mantener

En lo que respecta a los envíos (*forwarding*), los switchs IP+ATM utilizan hardware ATM convencional y la clásica comunicación de etiqueta (*label switching*).
Una funcionalidad adicional de la componente de control es la denominada de asociación y distribución de las etiquetas (*label binding*) a las distancias definidas por el protocolo de encaminamiento IP (asociaciones que en el modelo overlay, eran tarea de la señalización ATM).

La diferencia principal entre las varias propuestas por la integración IP+ATM, hace referencia al mecanismo de asignación de la etiquetas. Son dos las aproximaciones utilizadas:

- modelo *data-driven* (Ipsilon Networks, Toshiba)
- modelo *control-driven* (Cisco, IBM, Ascend)

En el modelo *data-driven* las etiquetas vienen asociadas y distribuidas solamente cuando viene individualizando, por los switch IP+ATM, un flujo de los paquetes IP de “larga” duración.
En el modelo *control-driven*, por su parte, las etiquetas vienen asignadas y distribuidas a través de las elaboraciones del protocolo de enrutado IP, independientemente de la llegada de trafico de datos. Esto es también utilizado en el estándar MPLS.

D.2.3.1. Ventajas e inconvenientes de este tipo de soluciones

La ventajas que supone el trabajo con etiquetas y la idea que tras ella se ha elaborado, supone un gran avance respecto al modelo *overlay.* Entre las grandes ventajas existentes, se puede destacar:

- La inteligencia para la asignación de caminos se concentra en la frontera de la red

- El reenvío lo puede realizar un conmutador (no son necesarias funciones de encaminamiento paquete a paquete en los nodos intermedios)

- La asignación de un paquete a un camino particular se puede basar en información que no está presente en la cabecera (por ejemplo, criterios de gestión de red)

- Permite la definición de rutas explícitas desde el sistema de gestión

De todos modos, este tipo de características no dejan de ser teóricas hasta que se sacan del papel y se pone en práctica. En principio, estas ventajas, estas innovaciones, debían proporcionar los cambios deseados por las grandes empresas y por los promotores de las grandes soluciones presentadas a finales de los ’90.

D.2.4. Modelo *overlay* vs. modelo *peer-to-peer*

Las diferencias principales entre los dos modelos, en términos de funcionamiento, pueden ser resumidos de la siguiente manera:

- En el modelo *overlay* el PVC entre dos routers vienen realizados a través de la señalización mientras que en el modelo *peer* viene realizado a través del protocolo de asociación y distribución de las etiquetas.

- En el modelo *overlay* coexisten dos protocolos de enrutado independientes: el IP y el ATM; en el modelo *peer* las distancias son decidas por un único protocolo de enrutado, el IP

- En el modelo *overlay* un router origen (por ejemplo, O), en lo que respecta al protocolo IP, tiene como adyacente el router destino (D), mientras que en el modelo paritario tiene como adyacente un switch IP+ATM

- En el modelo *overlay* el paquete IP viene segmentado y reensamblado en cada router del camino, mientras que en el modelo peer viene segmentado en el router frontera de entrada y reensamblado en el router frontera de salida.

El aspecto más visible, en el paso del modelo overlay al modelo paritario es la incorporación de inteligencia de enlutado IP en los switch ATM, con la consiguiente eliminación del enrutado ATM. Esto provoca la reducción del número de mensajes IP y la consiguiente eliminación de los problemas de estrés provocados por el enrutado IP.

Incluso con las grandes mejoras presentadas por el modelo peer, existen puntos negativos en respecto al anterior caso e incluso puntos no mejorados por esta nueva propuesta. Son por ejemplo:

- El espectro de banda introducido para el trasporte ATM (Cell Tax)
- La escalabilidad de la interfaz SAR ATM, difícil de realizar a velocidad superiores a 622 Mbps
- La falta de interpolabilidad entre la distintas soluciones

Sobretodo a causa de este último punto, se optó por la búsqueda un estándar universal para reducir la falta de mercado que tenía. De esta manera se quería llegar a un proceso de estandarización de las infraestructuras de redes que pudiera otorgarle a las redes las exigencias del mercado.

ANEXO E. MPLS. EL PRESENTE DEL FUTURO

El modelo paritario, puso sobre la mesa un abanico de nuevas posibilidades y de nuevas propuestas para poder incorporar a las maltratadas redes *backbone*. MPLS, como niño prodigio de ese modelo, se pudo situar a la cabeza de la vanguardia en infraestructuras de red.

Durante este anexo, podremos realizar un "viaje" por las singularidades más importantes de MPLS, y conocer un poco más sobre esta tecnología. Este anexo, aporta un recorrido, que ayuda a entender mejor el Capítulo 3.

E.1. Del modelo paritario a MPLS

La idea de MPLS parte del modelo paritario o integrado IP/ATM, tal y como se puede ver en la figura D.1. De cara a su posible implementación ya se adelantó que la IETF, ideó este modelo como propuesta de estándar universal, para poder obtener el hilo conductor que pudiera englobar las anteriores propuestas.

Los objetivos generales de ese proceso de estandarización, no se basaba únicamente en este aspecto, sino que se sustentaba en los siguientes puntos:

- desarrollar las ideas a partir del modelo paritario
- funcionalidad con diferentes tecnologías de nivel 2 (no sólo ATM)
- incrementar las prestaciones de los routers
- hacer evolucionar el enrutado IP a nuevas funcionalidades, como por ejemplo la posibilidad de "ingeniería del tráfico"
- otorgar a las redes IP más escalabilidad, o sea en posición de despachar tráficos de grandes dimensiones y de ofrecer servicios como por ejemplo VPNs a un conjunto de clientes grande y diferenciado
- soportar los modelos de QoS desarrollados en el ámbito IETF (como se hace referencia en los RFCs 1633, 2212 y 2211)

La idea base de MPLS es introducir en las redes IP el concepto de "conmutación de etiqueta" típico de las redes a conmutación de paquetes *orientadas a conexión* (X.25, Frame Relay, ATM) y por lo tanto de introducir en un ambiente *no orientado a conexión*, como el de IP, el concepto de *conexión virtual*. Este concepto, se consigue asociando a todos los paquetes una pequeña identificación de longitud fija, etiqueta (*label*), que los dispositivos de la red puedan utilizar para efectuar un encaminamiento veloz. De todas formas no se puede considerar a MPLS como un nuevo protocolo de enrutado, aunque sí como una nueva técnica de envío de los paquetes IP.

Uno de los muchos puntos fuertes de MPLS es su flexibilidad, además de no tener la necesidad de asociarse a una tecnología de transporte en particular (a diferencia del modelo paritario, basado en ATM). Por otra parte, MPLS es también muy genérico en lo que a contenidos del transporte se refiere, además de un grado de transporte para cualquier tipo de contenido, sea, por ejemplo,

un paquete de nivel 3 (IPv4, IPv6, IPX, etc.) o una trama de nivel 2 (PPP, Ethernet, *Frame Relay*, ATM, etc.). En cierto modo se puede decir que MPLS es totalmente inconsciente sobre qué transporta. Esto explica el adjetivo de Multi-protocolo adherido a su nombre (características ilustradas en la figura E.1).

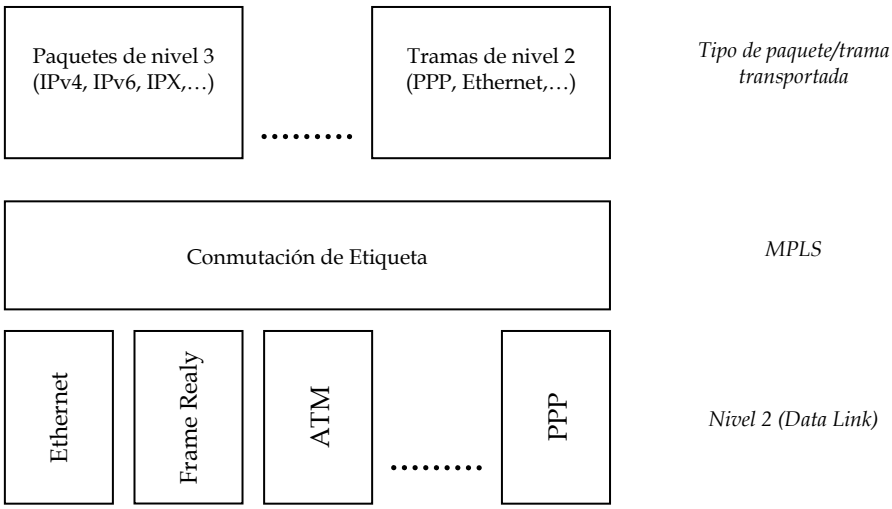


Fig. E.1: Niveles de actuación de MPLS

Teniendo en cuenta esta flexibilidad, su situación en el modelo de capa OSI/ISO, sería difícil. Tal y como se muestra en la figura, no se puede colocar ni en el nivel 2, porque es independiente del protocolo utilizado, y no puede ser asignado como de nivel 3 porque le restan las funcionalidades de enrutado y encaminamiento que el modelo OSI exige para este nivel. Por lo tanto, MPLS no es clasificable en un modelo de OSI, pero incluso así, ha tenido una gran aceptación en los ambientes de redes de telecomunicaciones.

E.2. Los mitos y sus realidades

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS.

Primero. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a *routers* de *backbone* de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel en la mitad de los años '90, los progresos en la tecnología del silicio (a través de ASIC – *Application Specific Integrated Circuits*) permite efectuar una lectura de las tablas de enrutado IP a velocidades comparables a las de una tabla de encaminamiento ATM. Con lo que echa por tierra esta posibilidad.

Segundo. Ha habido quien pensó que el MPLS perseguía eliminar totalmente el encaminamiento IP convencional. Este no ha sido nunca un objetivo de Grupo de Trabajo de MPLS, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en la Internet por los siguientes motivos:

- Se requiere examinar la cabecera de los paquetes para su filtrado en los cortafuegos de acceso a las LAN corporativas y en los límites de las redes del proveedor. Lo que sugiere que es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad.

- No es probable que los sistemas finales (*hosts*) implementen MPLS. Esto conlleva la necesitad de enviar los paquetes a un primer dispositivo de nivel 3 que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final.

- Las etiquetas MPLS tienen solamente significado en el dominio MPLS (es imposible mantener vínculos globales entre etiquetas y *hosts* en toda la Internet). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde enviarlo.

- Del mismo modo, el último router del dominio MPLS deberá necesariamente examinar el paquete a nivel 3 para entregar el paquete al destino externo de la red.

E.3. Apunte inicial

Después del largo camino recorrido hasta el momento, no sabemos demasiado de esta tecnología. A partir de este momento, se abrirán las puertas a algunas de las preguntas sobre el funcionamiento de MPLS.

Por lo pronto, una de las grandes peculiaridades de MPLS es que consigue transformar una red *no-orientada a conexión* en una red *orientada a conexión*. Gran parte de la culpa la tiene la utilización de la conmutación de etiquetas, que formará parte del estudio en los siguientes puntos.
Este mecanismo, a modo de resumen, se podría englobar en cuatro pasos fundamentales:

- Clasificación: identificación del flujo de tráfico al cual pertenece el paquete
- Imposición de etiqueta o pila de etiquetas: asociación de una o más etiquetas al paquete y de poca información más
- Inserción en la red: envío del paquete al interior de la red MPLS basándose solamente en el valor de la etiqueta (la más externa para el caso de pila de etiquetas)

- Eliminación: Supresión de la etiqueta a la salida de la red MPLS

Para llevar a cabo este proceso, los routers de la red deben soportar MPLS en todas las interfaces, a excepción de las más próximas al usuario-cliente de la red, por las razones explicadas en el punto anterior.

E.3.1. Algunas definiciones

A continuación algunas pequeñas definiciones sobre siglas muy usadas, que ayudarán a comprender un poco más las explicaciones.

- FEC (*Forwarding Equivalence Class*): Clase de Envío Equivalente, es un subconjunto de paquetes IP que son tratados de la misma manera por un router. Podemos decir que en el enrutado convencional, cada paquete está asociado a un nuevo FEC en cada salto. En MPLS esta operación sólo se realiza la primera vez que el paquete entra en la red.

- Etiqueta: un identificador de longitud corta y constante que se emplea para identificar una FEC, normalmente con carácter local. En el caso de ATM, las etiquetas se codificarán dentro de los campos vpi - vci de los paquetes ATM.

- LSP (*Label Switched Path*): Camino Conmutado de Etiquetas es el camino compuesto por uno o más routers dentro de un nivel jerárquico por el que un paquete perteneciente a un determinado FEC circula. Todos los paquetes pertenecientes a un mismo FEC circularán siempre por el mismo camino LSP.

E.4. Funcionamiento y componentes de red

Básicamente, los puntos más importantes a tratar en este punto son tres:

- El funcionamiento del envío de los paquetes y por lo tanto, de la conmutación de etiquetas
- La estructura y el rol de los diferentes routers MPLS de la red
- La arquitectura de la red

E.4.1. La conmutación de etiquetas

MPLS utiliza, para el envío de los paquetes, un paradigma muy conocido en las redes de conmutación de paquetes, característico de los estándares *orientados a conexión*: la *conmutación de etiquetas* (*label switching*). Con MPLS este concepto viene introducido por primera vez en las redes *no-orientadas a conexión*, como por ejemplo las redes IP.

La base de esta conmutación está en la asignación e intercambio de las etiquetas, para permitir establecer los denominados caminos LSP. Estos caminos no son más que circuitos virtuales que siguen por la red todos los paquetes asignados a la misma FEC. Los LSP son simples (se establecen para un sentido del tráfico en cada punto de entrada a la red); para el tráfico dúplex, requiere dos LSP. Cada LSP se crea a base de concatenar uno o más saltos con el intercambio de las etiquetas, de modo que cada paquete se envía de un LSR (router MPLS) a otro, a través del dominio MPLS.

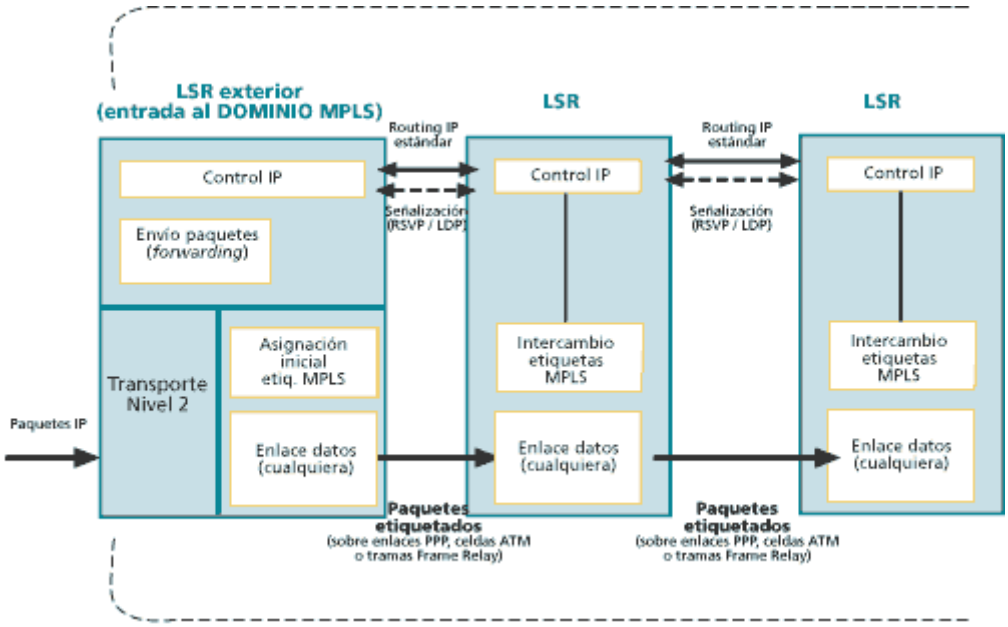


Fig. E.2 Esquema funcional del MPLS

El la figura superior (**Fig. E.2**) se pueden distinguir las distintas operaciones que se llevan a cabo en un domino MPLS. La gran diferencia se encuentra, como veremos en el punto siguiente, en que los LSR más exteriores de la red, deben tener al menos una interfaz de nivel 2. Se puede observar también que MPLS separa el *routing* y en *forwarding*, como sucede en otras soluciones de conmutación multinivel. Del mismo modo, el envío se implementa mediante el intercambio de etiquetas entre en los LSR.

Para poder entender un poco más todo este proceso, este ejemplo del *Boletín 53 de Rediris* (**fig. E.3**) ayudará. Como se puede observar, el LSR de entrada recibe un paquete sin etiquetar cuya dirección de destino es *212.95.193.1*. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo *212.95/16*. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el

siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por *routing* convencional. Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP.

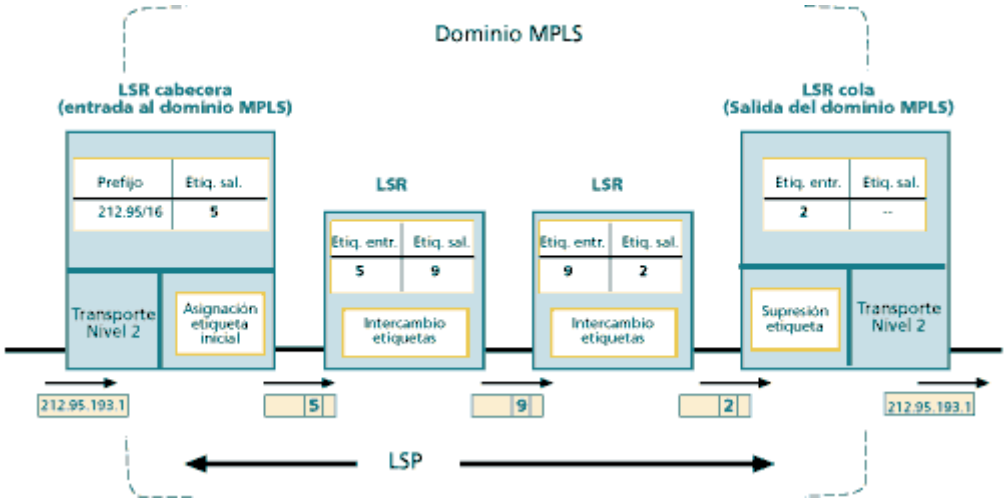


Fig. E.3 Ejemplo de envío de un paquete por un LSP

Con todo esto, podemos decir que, a grandes rasgos, una red MPLS opera del siguiente modo:

1. El paquete recibido por el router de entrada de la red MPLS es clasificado (asignándole a una FEC), y acto seguido etiquetado y enviado al router siguiente.
2. En el siguiente router, el encaminamiento del paquete se decide leyendo sólo la información de la etiqueta del nivel más elevado; el router consulta una tabla que asocia el valor de la etiqueta según las instrucciones contenidas en la tabla y acto seguido el paquete es enviado al siguiente router, continuando así el camino LSP, salto a salto.
3. Cuando el paquete llega al último router del recorrido, éste borra la etiqueta y envía el paquete teniendo en cuenta el contenido de otra etiqueta, y si no hay más etiquetas, partiendo de la información del protocolo transportado.

Una de las situaciones más ventajosas que nos proporciona este tipo de tecnología es que la clasificación de los paquetes sólo se efectúa en el router de entrada. El resto de veces que ese paquete pase por un router, lo único que se observará será la etiqueta más exterior.
Esto simplifica mucho los procesos de envío ya que los routers intermedios no pierden tiempo en cálculos y procesos complejos. Lo que conlleva una mayor velocidad y por lo tanto menor posibilidad de congestión.

Otro punto reflejado en esta explicación del proceso, es que el "modus operandi" es independiente del contenido transportado. Lo que refleja la gran versatilidad de aplicaciones que pueden utilizar MPLS.

E.4.2. Arquitectura de los routers MPLS

La arquitectura de los routers MPLS, llamados LSR (*Label Switching Router*) sigue la tradicional separación funcional de los routers convencionales, en *componente de control* y *componente de envío*.

- Componente de control: comprende todas las funciones "inteligentes" del LSR: los protocolos y algoritmos presentes en un router convencional para el intercambio de las informaciones de enrutado con los otros LSR y para la construcción de la tabla de enrutado.
  La información de enlace de etiquetas, como se mostraba en la figura E.2, es comunicada mediante varios mecanismos, destacando el Protocolo de Distribución de Etiquetas (*Label Distribution Protocol* – LDP). En muchos casos se emplean otros protocolos diferentes para este cometido, como pueden ser: RSVP, PIM y actualmente se baraja mucho la utilización explicita de BGP.

- Componente de envío: es mucho más simple que la de un router convencional en cuanto a procedimiento de envío. Esta se basa en la simple conmutación de etiquetas y también de otras simples operaciones de la pila de etiquetas. La tabla que se construye a partir de la información de encaminamiento que proporciona la componente de control, es utilizada por este componente para poder enviar los paquetes. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que son relacionadas con la correspondiente etiqueta e interfaz de salida.

Existen diversos tipos de LSR, diferenciados por el rol que ejercen en la red:

- Edge-LSR
- LSR de transito
- ATM-LSR
- ATM Edge-LSR

Un Edge-LSR es aquel situado en la frontera de la red y tienen por lo menos una interfaz *non-MPLS*. Por su parte, los LSR de tránsito son aquellos que tienen todas las interfaces MPLS y que se encuentra en el interior del domino.
Los otros dos LSR restantes son máquinas iguales que las anteriores pero adaptadas para trabajar en MPLS de nivel 2.

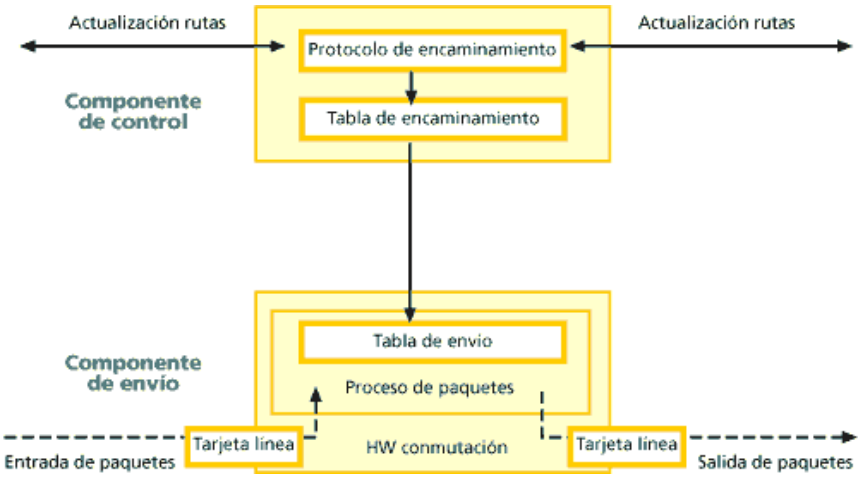


Fig. E.4 Componente de control y de envío de etiquetas

E.4.3. Arquitectura de la red MPLS

Una red de este tipo tiene una arquitectura que no difiere de una red tradicional si no fuera por el tipo de routers utilizados, que obviamente deben soportar MPLS. En ellas los routers pueden ser clasificados en:

- router de acceso: son los router a los que se conectan, a través de conexiones directas (PVC ATM o Frame Relay, u otro) a las redes de los clientes.
- router de transito: son los routers internos de la red, que desarrollan principalmente funciones de distribución del tráfico

Un conjunto de routers de acceso (edge_LSR) y el router (o los routers) de transito (LSR) a los cuales estos están conectados, se les llama PoP (*Point of Presence*). En las redes de grandes dimensiones un PoP consiste normalmente de más Edge-LSR, y de un LSR.

En la siguiente figura (**Fig E.5**), a modo de resumen, se muestra un ejemplo de típica estructura de red MPLS, con los distintos procesos que se llevan a cabo en su interior.

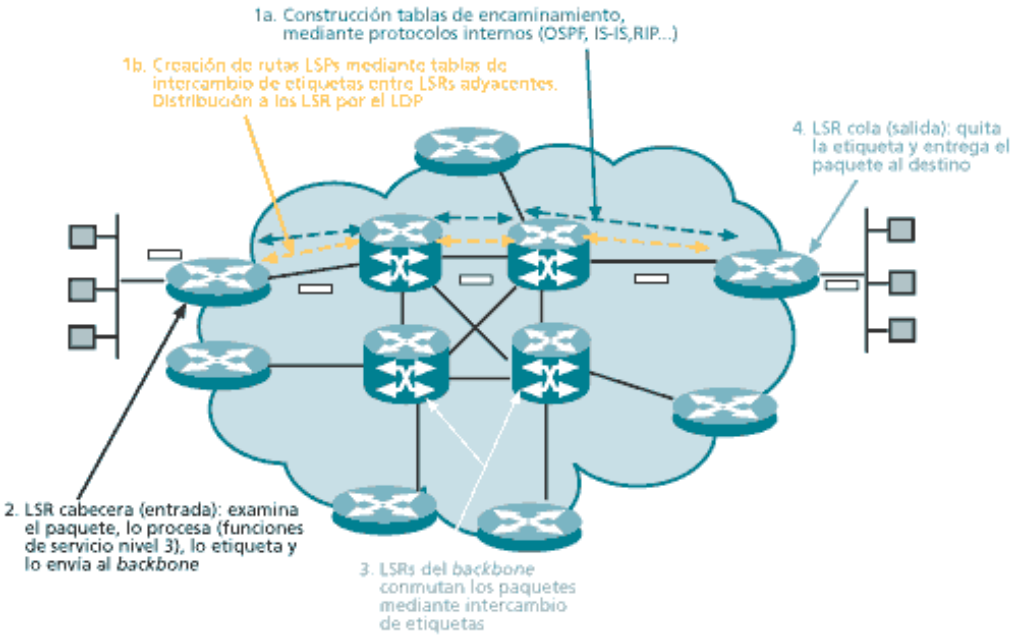


Fig. E.5 Estructura de red MPLS

E.5. Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico: El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén sobreutilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. El problema recae en que los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente (RIP, OSPF, etc.). Estos caminos no están adaptados a los requisitos de los flujos, en cuanto a QoS se refiere, ni a la "vida" de los nodos (que pueden estar provocando un cuello de botella). Con la ingeniería del tráfico se consigue trasladar determinados flujos a otros enlaces menos congestionados (aunque sean de más saltos).
  Cabe destacar, que con este tipo de aplicaciones el administrador puede establecer rutas explicitas para servicios especiales de QoS, y obtener estadísticas del uso de LSPs para evitar cuellos de botella y cargas excesivas de enlaces.

- Diferenciación de niveles de servicio mediante clases (QoS): MPLS está diseñado para poder cursar servicios diferenciados, según el modelo *DiffServ* del IETF. Este modelo define una variedad de mecanismos para

poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades.
MPLS se adapta a través del campo *EXP* incluido en las etiquetas, con el que pueden propagar la clase de QoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR.
- Entre cada par de LSR exteriores se pueden situar múltiples LSP, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda.

- Servicio de redes privadas virtuales (VPN): Las VPN proporciona conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.
  Este tipo de servicios se basan en las PVC de redes como *Frame Relay*, pero con la mejora de una gestión y configuración mucho más sencilla.

Durante todo el anexo se ha estado presentado todos y cada uno de los componentes que se pueden encontrar en un domino MPLS simple. Lo más gratificante de todo ello, es que consiguen mejorar las prestaciones de los modelos ATM e IP más simples, o las asociaciones de ellos.

ANEXO F. VPN Y SUS SOLUCIONES EMERGENTES

Las redes virtuales han estado presentes en las telecomunicaciones desde sus primeros pasos. La idea principal de este tipo de tecnología era asociar puntos distantes geográficamente de manera que parecieran estar en el mismo punto. Sin duda alguna, las grandes empresas (clientes) y los proveedores de servicios no querían arriesgarse a mermar la privacidad de los datos enviados. A finales del siglo pasado, las VPNs se eligieron como la gran apuesta de futuro, y un aliado perfecto para MPLS para igualar las características ofrecidas en infraestructuras ATM con PVC y a menor escala, también con VPN.

El camino que lleva recorrido la tecnología VPN, no tiene ni punto de comparación con lo que falta. Desde hace pocos años, un sinfín de nuevas propuestas siguen surgiendo para satisfacer, como no, las necesidades de los grandes clientes y, por que no decirlo, las grandes carencias que demostraba en seguridad.

Durante este anexo se mostrarán las 3 grandes propuestas que se barajan: L1VPN (nivel 1), L2VPN (nivel 2) y L3VPN (nivel 3). De entre ellas, la de nivel 1 es la que parte con desventaja, mientras que las de los niveles 2 y 3 solventan algunas unas carencias que a la otra le resta.

F.1. Historia de las VPNs

El término “red privada virtual” es muy amplio y puede llegar a tener un significado distinto para cada persona. No existe por ello una clara definición sobre su emplazamiento dentro de las infraestructuras de telecomunicaciones.
Ante esta traba, una definición generalista podría ser la mejor manera de empezar. Por lo tanto, una VPN se podría definir como sistema para crear una comunicación privada entre distintos puntos, utilizando una *backbone* que es compartida por otros tráficos no destinados para esa comunicación.

Inicialmente, las VPNs consistían en redes privadas interconectadas por dispositivos de marcado manual (dial-up) o dedicado, sobre redes alquiladas a las compañías de telefonía. De esta manera las grandes empresas e instituciones disponían de líneas dedicadas para unir los distintos emplazamientos no próximos demográficamente.

A finales de los ’70 se desarrolló el sistema X.25 (*RFC 1356*), como forma de conexión virtual (VC) de comunicación de paquetes en una WAN. Este estándar permite la separación a nivel lógico de diferentes canales de usuario, sobre conexiones compartidas. De manera que los diferentes usuarios beneficiarios de este sistema, tienen la sensación de disponer de una conexión dedicada cuando en realidad es compartida por distintos canales, para una o diversas organizaciones-clientes.

A comienzos de los ’80, X.25 ofrecía a las organizaciones la posibilidad de utilizar VPN en redes con los protocolos más utilizados en aquellos años (SNA, DECnet), de la misma manera que hoy se utiliza TCP/IP. La llegada de la alta velocidad con Frame Realy y ATM en los 90 proporcionó a las VC velocidades de 155 Mbps.

La topología de estas VPNs consistía en la unión de diferentes routers clientes IP interconectados con mallas parciales o totales de VCs Frame Relay o ATM, a otros dispositivos cliente (CPE - *Customer Premise Equipment*). Mientras tanto, la triple W (www) se hacía cada vez más popular y, las empresas inundaban sus oficinas de ordenadores conectados entre sí y hacia un exterior lleno de nuevas oportunidades de ventas gracias a Internet. Esta creciente demanda propició el auge de la tecnología IP VPN, que facilitaba la posibilidad crear comunicaciones a través de Internet *site-to-site* y *user-to-site*.

Las primeras VPNs desarrolladas sobre redes IP trataron dos segmentos del mercado específicos:

- *Virtual Private Dial Networks* (VPDN): permitía establecer una conexión entre un usuario y el *gateway* de la empresa a través de una sesión PPP. Esta sesión PPP se establecía a partir de la combinación de un enlace de datos *dial-up* establecido con el router frontera del proveedor de Internet, y un túnel VPN desde el router frontera del ISP hasta la *gateway* de la empresa (o punto final).
  Para establecer la conexión, se requería autenticación de cliente y la negociación del protocolo a utilizar. Algunos de estos protocolos podían ser: PPTP (*Point-to-Point Tunneling Protocol*), L2F (*Layer 2 Forwarding*) o el más utilizado L2TP (*Layer 2 Tunneling Protocol*).

- IPsec VPN: destinado a cumplir los requisitos de integridad de datos, autenticación y privacidad que piden las empresas en sus comunicaciones a través de la red pública (Internet). Para conseguir este nivel de seguridad, el cliente (o proveedor, gestionando los routers CPE) construye túneles IPsec sobre la Internet para interconectar los CPEs. Utiliza una variedad de protocolo de intercambios y autenticación en los puntos finales del túnel para autenticar y encriptar los paquetes de datos de los usuarios enviados a través de la red compartida.

Para los proveedores de servicios y para los clientes de estos, seguían insistiendo en que MPLS ayudado por el sistema de VPN, debía satisfacerles en los siguientes puntos:

- Eficiencia de la red central de interconexión de paquetes: intentar encontrar una solución para evitar las congestiones, sobrecargas, etc.; tal y como ocurría en redes mal gestionadas de ATM y Frame Relay.

- Gran automatización en la creación y gestión de VPNs: pedían eliminar o aliviar la complejidad de la creación de las PVCs en infraestructuras como ATM i Frame Relay.

- Habilidad para ofrecer diversos servicios sobre la misma infraestructura: Las empresas de servicios querían conseguir con esto, la llamada convergencia de los servicios o lo que es lo mismo, conseguir una infraestructura de red de multiservicios.

Sin hacer caso omiso de estas "propuestas de mejora", en Mayo del 2000, el Grupo de Estudio 13 de la ITU-T empezó a definir los requisitos de las VPN y clasificó las distintas propuestas para servicios de nivel 3 sobre MPLS. Al año siguiente la IETF creó el Grupo de Trabajo PPVPN (Provider Provisioned VPN) con el objetivo de estandarizar las soluciones que surgieran de los niveles 2 y 3. Con ello, nadie ha parado de trabajar, e incluso hoy se buscan alternativas a las VPNs para algunas situaciones. Incluso, añadir mejoras de antiguos protocolos a esta tecnología con el fin de consolidar las propuestas que en su día hicieron las grandes empresas.

F.2. Modelos de referencia VPN

Habiendo leído el título de esta sección, seguro que más de un autor se tiraría de los pelos. No es sencillo clasificar las diferentes soluciones existentes de VPNs, y aún menos destacar una de ellas sobre el resto. Esto mismo lo plantea Tiziano Tofoni en su libro "MPLS. Fontamenti e applicazioni alle reti IP". Tofoni no destaca por exponer una clasificación revolucionaria, sino por darnos algunos criterios que permiten hacer distintas clasificaciones.

Estos son:

- El modelo de comunicaciones:
  - *Intraempresarial*, o comunicación exclusiva entre sucursales; creando de esta manera una Intranet
  - *Interempresarial*, o comunicación entre distintas empresas; estableciendo así comunicación de Extranet
  - VPN Dial-up, que es un modelo que prevé la comunicación desde usuarios en movimiento

- La modalidad de transporte de las informaciones de los Clientes sobre la red pública:
  - VPN *overlay*, donde la red pública es una simple red de transporte
  - VPN *peer-to-peer*, donde la red pública intercambia con los Clientes también información de enrutado

- La topología lógica de la red:
  - Estrella
  - Doble estrella, que es la estrella pero con redundancia
  - Malla

- Híbrida, que combina la topología de estrella y de malla

De entre todos estos criterios, normalmente los autores utilizan la modalidad de transporte para explicar los tipos de soluciones que existen. Aunque esta es una buena manera, aún existe otra, que últimamente está teniendo mucha aceptación. El criterio que se utiliza en este caso es clasificar según los gestores de la red y por lo tanto, los puntos de ésta donde se colocan los dispositivos especializados. El resultado de esta clasificación son dos modelos generales: *PE-based VPN* (*PE - Provided Edge*) y *CE-based VPN* (*CE - Customer Edge*).

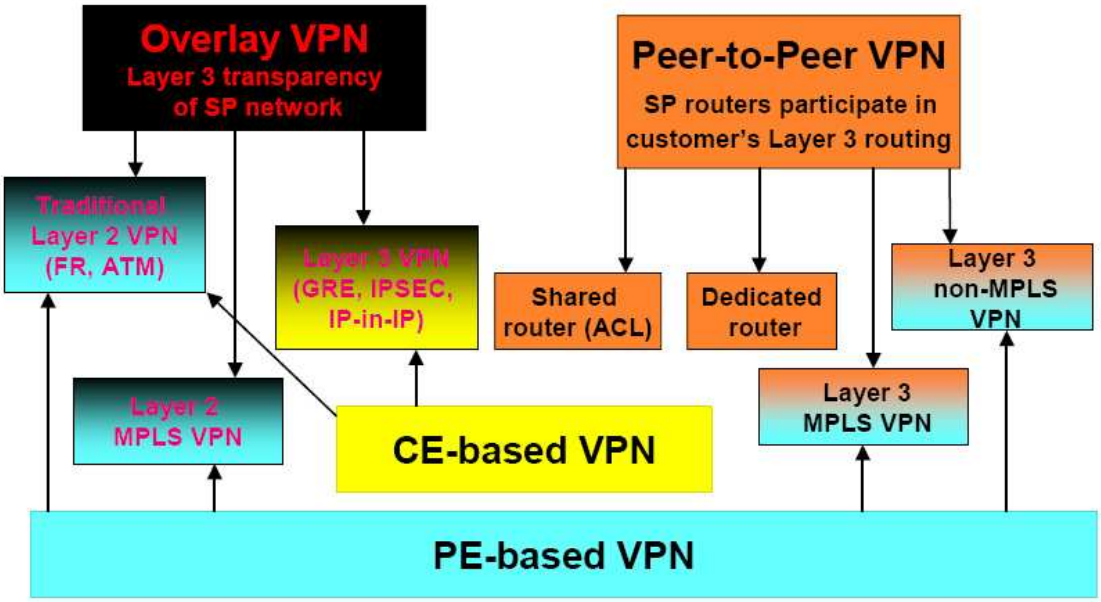


Fig. F.1 Taxonomía de las VPN

La figura F.1 ayuda a entender la relación entre estas propuestas. Se pueden observar las relaciones entre las distintas soluciones y las capas sobre las que trabajan.

Existen dos puntos destacables en relación con las definiciones de la mayoría de los autores. El primero es que normalmente se relacionan directamente los modelos CE-Based VPN con el overlay, y PE-based VPN con el peer-to-peer, eliminando la relación entre overlay y PE-based VPN porque indican que es una opción menos adecuada. Lo cierto es que tanto una como la otra son aún caso de estudio en la IETF, pero en gustos no hay nada escrito.

El segundo de los puntos que me gustaría destacar es la inexistencia de la solución L1VPN. Pero en este caso, aunque ésta opción también se está estudiando actualmente no es un error de los autores puesto que no hay aún demasiada información al respeto y lo que acaban haciendo la mayoría es un pequeño apunte al respecto.

Después de revisar una serie de trabajos, y observando que la gran mayoría de los estudios actuales utilizan los modelos CE y PE-based VPN para explicar a fondo las redes virtuales, la clasificación de las soluciones se hará a partir de estos dos modelos.

De todas maneras, los modelos overlay y peer-to-peer son muy parecidos a los explicados para IP/ATM, y no ayudaría a obtener una visión más amplia de la topología de las VPN, lo que hace a la opción escogida algo más suculenta.

A partir de ahora, la figura F.2 ayudará a entender la taxonomía de los tipos de VPN IP que existen, clasificándolas según la conectividad que existe entre las partes: site-to-site, o user-to-site. Aunque, en realidad sólo PE y CE-based VPN serán comentados.

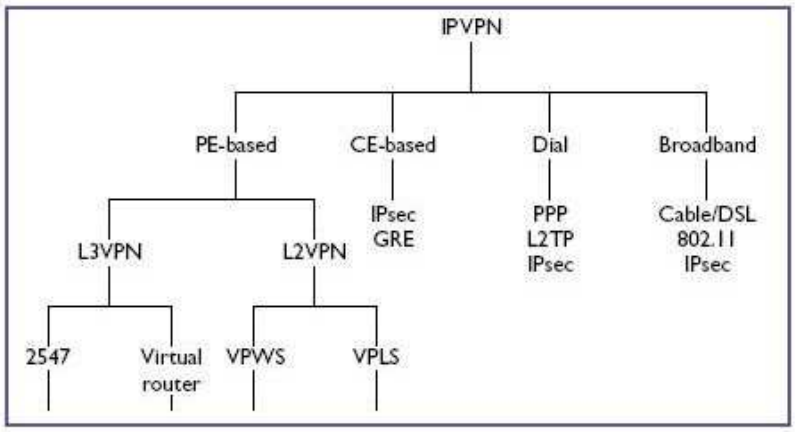


Fig. F.2 Taxonomía de las VPN según conectividad

F.2.1. Modelo PE-based VPN

Tanto el modelo CE como el PE basados en VPNs, son redes site-to-site. Esto significa que son modelos creados para unir puntos finales, y que utilizan una red central para intercambiar los paquetes. No es el único punto en común, pues si se observan las figuras F.3 y F.4, puede notarse que los dispositivos CE (*Customer Edge*) y PE (*Provider Edge*) son utilizados en ambos casos. La gran diferencia, es la utilidad que se les da en cada uno de los modelos.

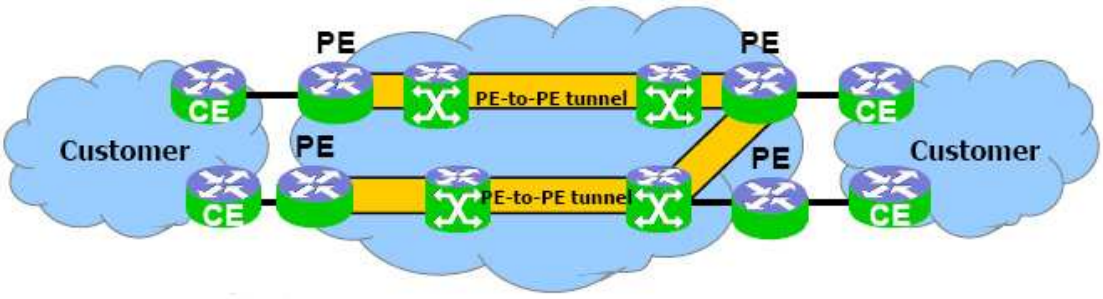


Fig. F.3 Ejemplo simple del modelo PE-based VPN

PE-based o Network-based VPN, se distingue por volcar a los PE toda la configuración y gestión de las VPNs creadas. Esto quiere decir que las VPNs tienen su principio y fin en las PEs, y que por lo tanto, lo único que deben hacer los clientes, es conectar su router frontera al PE más cercano.

Como se observa en la figura F.2, este modelo puede subdividirse en diversas soluciones: L3VPN y L2VPN. En realidad, también existe la opción de trabajar con una solución de nivel 1 (L1VPN), pero está aún por determinar.

Para poder direccionar los paquetes, el sistema de nivel 3 se guía observando la cabecera IP. En cambio, el L2VPN tiene en cuenta el nivel 2 (la dirección MAC, los identificadores de conexión VC, etc.) o la información de puerto.

F.2.2. Modelo CE-based VPN

Como se puede intuir, en este caso, todo el peso del control y la gestión de las VPN recaen en los CE. De esta manera, el proveedor de servicios no tendrá ninguna conciencia de la cantidad de VPNs que atraviesan la red, y de ningún esquema de enrutado o direccionamiento. Esto quiere decir que sólo ve paquetes IP que atraviesan la red de CE a CE.

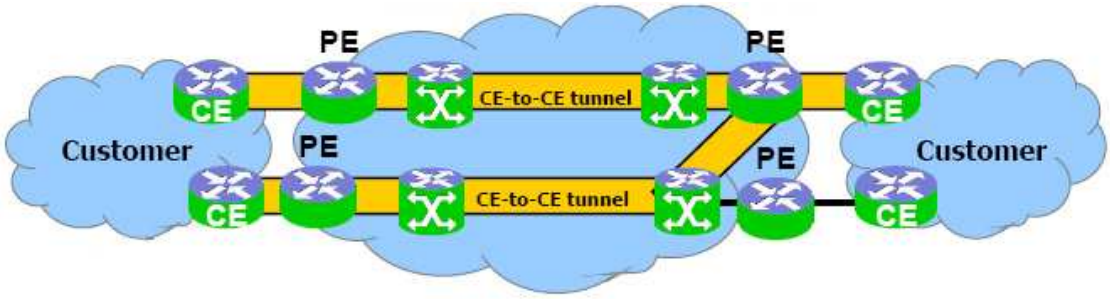


Fig. F.4 Ejemplo simple del modelo CE-based VPN

En este caso, sólo se tiene en cuenta el nivel 3 para VPN, y no hay ningún estudio o pretensión de estandarización de otros niveles. Aunque esto no quiere decir que no se pueda trabajar sobre ellos.

F.3. L1VPN

No es que exista una gran bibliografía referente a esta solución. La verdad es que más allá del año 2004 poca cosa se puede encontrar.

Es cierto que la ITU-T SG 13 tiene en cuenta esta opción, pero la gran mayoría de investigadores del sector tienen puestos sus ojos en capas más altas. El tiempo dará la razón a unos o a otros (o a nadie), respecto a cuál de los 3 niveles se adapta mejor a las exigencias del sector. Pero sin duda, me han

mantenido entretenido observando los movimientos de ideas e intenciones de todos ellos.

F.3.1. Cuatro pinceladas

A día de hoy las grandes redes se basan en SONET/SDH (Synchronous Optical NETworks / Synchronous Digital Hierarchy), controladas y gestionadas por EMSs (element management systems) y NMSs (network management systems). Estos tipos de sistemas de gestión tienen un alto coste, y además se necesita mucho tiempo para poder hacer cambios en la red. Esto provoca que muchas de las oportunidades que se presentan de negocio no sigan adelante por las trabas de tiempo y dinero que supone.

Algunas de las iniciativas para mejorar esta situación pasan por tecnologías como el GMPLS (Generalizad MPLS) para el plano de control o PCEMP *(Path Computing Element Metric Protocol)* para mejorar el intercambio de rutas.
Para estas dos propuestas, L1VPN es la base para poder crear una red compartida de gran flexibilidad y que ayude a reducir los altos costes de las actuales arquitecturas de red.

La idea principal es otorgar a la red un conjunto de servicios para poder controlar mejor las operaciones, y así crear una red más al gusto del cliente. Poder ofrecer a los usuarios de la red, la posibilidad de tener el rango de direcciones que desee, sin que ello interfiera en otras redes y poder establecer una comunicación clara con otros clientes, como si no hubiera nadie más en la red compartida.

Si se puede conseguir todo esto, las nuevas aplicaciones y servicios llegarán solos, porque el proveedor de servicios no tendrá grandes dificultades para modificar la red si es el caso.

F.3.2. Particularidades

Con la incorporación de L1VPN en la red de transporte, se consigue la independencia de las redes de cada cliente. Se complace la idea de poder disponer de una red (virtual) propia pero sin que ello conlleve la creación de una nueva red físicamente (algo enormemente costoso). En otras palabras, para el cliente, el resto de redes (redes de otros clientes y la red transporte) permanecen invisibles.

Esto es posible porque para los usuarios del plano de transportes las capas más altas son transparentes, separándolo físicamente del plano de control. De esta manera los recursos de la red pueden ser dedicados a una sola VPN o compartirlos con múltiples VPNs (como se ilustra en la **Fig. F.5**).

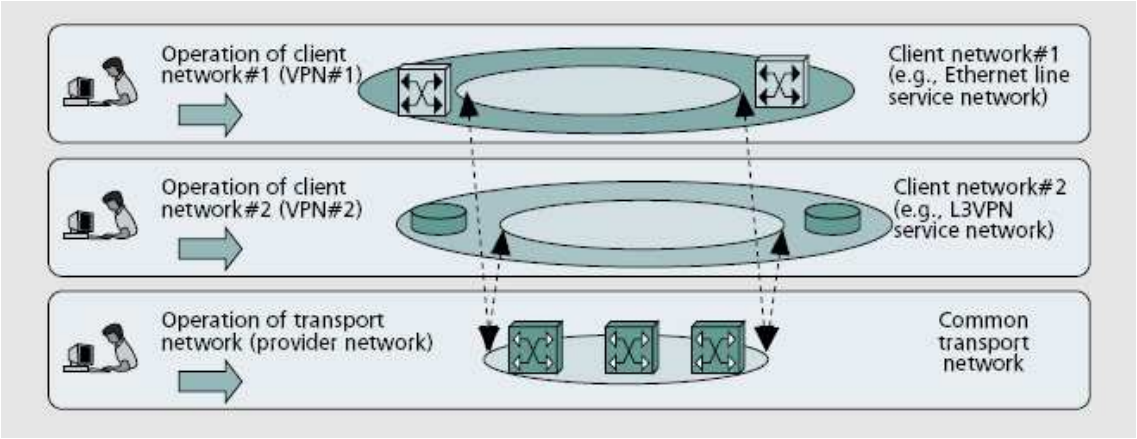


Fig. F.5 Concepto general de L1VPN

Este tipo de sistemas, facilita mucho el trabajo de los proveedores ya que la única responsabilidad de la red es la configuración de la infraestructura. Las conexiones entre clientes, son creadas dinámicamente lo que facilita la incorporación de nuevos servicios rápida y eficazmente.

En lo que respecta a las arquitecturas de red propuestas-existentes para L1VPN, sólo decir que a nivel general existen tres tipos de arquitecturas de control: Distribuida, Centralizada e Híbrida. Se pueden distinguir por la manera de distribuir la información de enrutado y de controles de conexión. En la versión centralizada es un dispositivo llamado PMS (*Provide Management System*) que gestiona esa información, dispositivo que en un sistema distribuido no se implica en esta tarea.

De todas formas, en cada una de las propuestas en que L1VPN toma parte, se exhiben distintas maneras de diseñar la infraestructura de red. Aún así, en todas las propuestas se puede observar que los elementos como el CE o el PE, permanecen presentes en todas ellas.

F.3.3. Documentos interesantes

Como resulta bastante difícil encontrar buen material al respecto, a continuación presento documentos donde se puede ampliar la información sobre L1VPN.

Para poder ampliar la información sobre modelos funcionales, requerimientos de la red y arquitecturas, el documento creado por *Tomonori Takeda*, *Ichiro Inoue*, *Raymond Aubin* y *Marco Carugi* es una gran opción:

- "*Layer1 Virtual Private Networks: Service Concepts, Architecture Requirements, and Related Advances in Standardization*"; de la revista "IEEE Communications Magazine" (Junio 2004)

El último draft que conozco referente a la propuesta de L1VPN con PCEMP, se puede encontrar por Internet fácilmente si se utilizan algunos de los siguientes datos:

- "*Framework of PCEMP based Layer 1 Virtual Private Network*" *(draft-choi-l1vpn-framework-02.txt);* Jun Kyun Choi, Dipnarayan Guha y Seng Kyoun Jo (Julio 2005)

Por último, el mejor documento que he encontrado sobre GMPLS asociado con L1VPN es el siguiente:

- "*Layer 1 Virtual Private Networks: Driving Forces and Realization by GMPLS*"; Tomonori Takeda, Deborah Grungard, Dimitri Papadimitriou y Hamid Ould-Brahim; IEEE Communications Magazine (Julio 2005)

F.4. L2VPN

Esta solución del nivel 2 está dirigida única y exclusivamente al envío de información a través de la red compartida y la creación de entornos de red privados para las empresas.

La gran diferencia entre ésta tecnología y los dos niveles restantes (1 y 3), es que su pasado es mucho más extenso. Hace más de 30 años que se oye hablar de las VPNs de nivel 2. Con la gran diferencia de que en el pasado, ATM y Frame Relay eran las grandes arquitecturas de red.

A día de hoy, las grandes empresas quieren obtener una tecnología que les cueste poco dinero, pero que les pueda permitir trabajar con un amplio abanico de servicios. Ante los ojos de los proveedores se presenta la oportunidad de trabajar con una red de nivel 3, y conseguir estos objetivos (al menos hasta cierto nivel). El problema es que no les gusta la idea de tener que hacer una gran inversión para trabajar a un nivel con el que "nunca" han trabajado.

Por lo tanto, entre otras cosas, la principal razón de la existencia aún de este tipo de tecnología y de la dedicación del grupo de trabajo exclusivo de la IETF, es la de satisfacer las demandas de aquellas empresas de servicios que no quieren cambiar a L3VPN (o a un posible L1VPN).

A su favor hay que decir, que si las L2VPN han estado en nuestras redes durante todos estos años, no seria por su poca efectividad, ¿no?.

F.4.1. Sus características

Esta tecnología puede soportar los mismos servicios que los dados por WAN y LAN de nivel 2. Por ello, un proveedor de servicios con L2VPN en su red puede

ofrecer un servicio entre sedes que soporte una red punto-a-punto FR o conexiones virtuales ATM; sin olvidar un servicio emulado de LAN Ethernet.

Por lo tanto, una de las características principales es que soporta el envío de *frames* de PDUs de Frame Relay, celdas ATM o frames de Ethernet. Algo que seguramente alegra mucho saber a los proveedores de empresas como las que se ha mencionado en la introducción de esta tecnología.

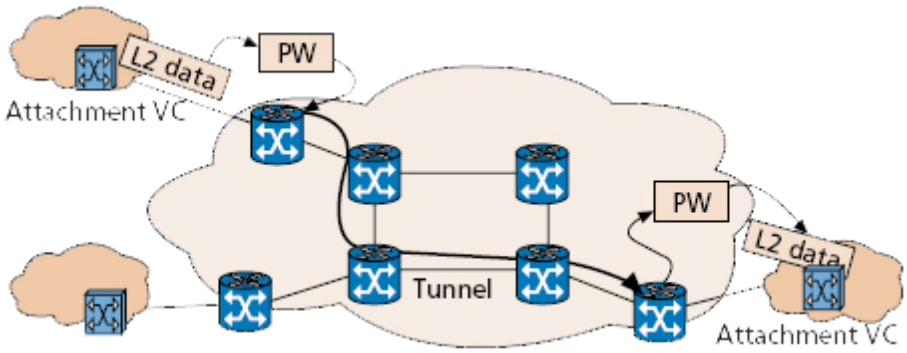
Cabe destacar que además del modelo punto-a-punto, también existe un modelo de servicios multipunto. Este normalmente se ofrece sobre Ethernet, que proporciona control de acceso al medio (MAC), para evitar la pérdida de información por la colisión de paquetes; también ofrece aprendizaje de direcciones y replicación de paquetes. De esta manera se consigue, que la WAN del proveedor aparezca como si los dispositivos de entrada estuvieran conectados a todos los dispositivos de la red.

De entre estos dos modelos, el más utilizado es el primero. Esto choca con la tendencia de L3VPN, que es la de proporcionar un servicio *point-to-cloud* (punto-a-nube).

F.4.2. La arquitectura de red

Si observamos la figura siguiente, podemos ver dos componentes que hasta ahora no habían aparecido. Podemos empezar con PW, que es la sigla utilizada para referirse a las conexiones denominadas *pseudo-wires*. Con ellas se consigue crear túneles a lo largo y ancho de las redes, emulando las antiguas conexiones de nivel 2.

Podemos observar también que aparece algo denominado Attachment VC. El elemento que crea estos acoplamientos es denominado AC (Attachment circuit). Estos elementos con conexiones (físicas o lógicas) que conectan un CE con un PE.



II.1.1

Fig. F.6 Arquitectura general de L2VPN

Siguiendo un poco el recorrido de las flechas de la figura F.6, podemos ver como el tráfico entrante de nivel 2 (ATM, Frame Relay, Ethernet VLAN) es

enviado a través de una PW concreta hacía su destino final en la red. Para ello, al payload original se le añade una cabecera PW, y acto seguido una cabecera asignada por protocolo del túnel (IPsec, GRE, u otros). De esta manera, la cabecera del payload no es leída durante todo el recorrido dentro de la red. Con lo que, es la cabecera PW que actúa como guía al salir del túnel y así poder encaminar el frame a su CE de destino.

Con esta solución, los usuarios de las redes no necesitan conocer todos los nodos de la red, únicamente el dispositivo frontera que tiene asignado. Esto ayuda a que la red pueda soportar un gran numero de Clientes, cada uno de los cuales con un gran número de usuarios. Sobretodo si tenemos en cuenta, que por cada túnel pueden viajar múltiples paquetes PW.

F.4.2.1. Los nodos PE y las pseudo-wires

Posiblemente estos sean los dos elementos de la red más importantes, ya que de ellos depende que los paquetes sean entramados en la dirección correcta.

Los nodos PE, pueden ser tanto routers IP como LSR (routers MPLS). Su rol en la red, es la de mantener actualizada la tabla de envíos de nivel 2, para poder escoger el camino correcto de cada frame. La tabla puede ser actualizada manualmente por los gestores de la red o dinámicamente por el protocolo de descubrimiento y replicación que utilice. La información que necesita para ello, dependerá siempre del servicio de nivel 2 que utilice la red.

Por otro lado las PW son las conexiones configuradas entre PEs, con un AC por cada una de ellas. Para que las conexiones PW puedan atravesar la red central, deben introducirse en los túneles que unen los diferentes nodos de la red. De esta manera, se puede decir que los túneles son los conductos de los conductos de los frames enviados. La información que tanto los túneles como los PW incluyen, son totalmente inútiles fuera de la red del proveedor, pero facilita que los clientes puedan disponer de todo el rango de direcciones que deseen para sus terminales.

F.4.3. Taxonomía de L2VPN

Tal y como se dijo en el apartado F.4.1, existen dos modelos de servicios distintos: punto-a-punto y multipunto (como se muestra en **Fig. F.7**). Lo que no se dijo, es que se les conoce como VPWS y VPLS respectivamente. Son dos modelos que pueden ofrecer el mismo abanico de servicios porque ambos pueden trabajar tanto en redes IP como en redes MPLS.

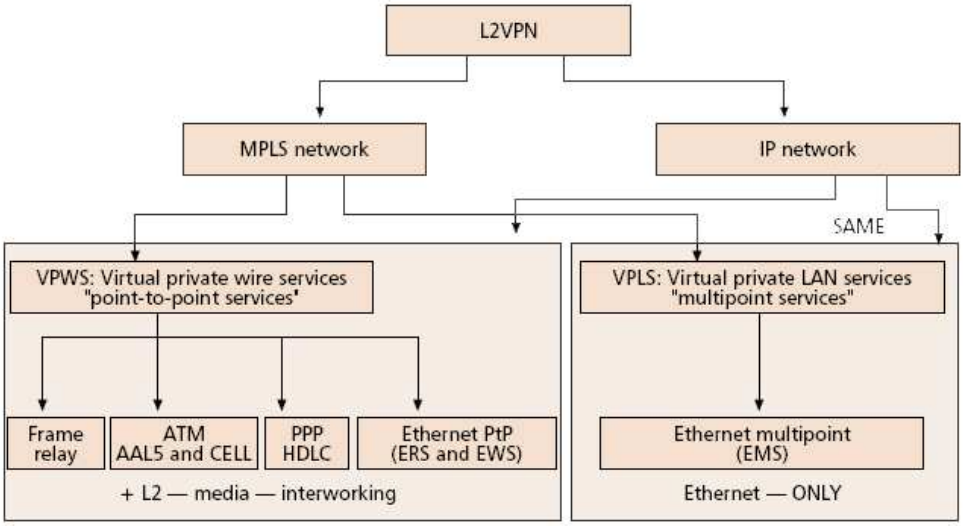


Fig. F.7 Taxonomía de L2VPN

F.4.3.1. VPWS

Virtual Private Wire Services (VPWS) es el alumno menos aventajado de los dos, ya que la mayoría de investigaciones se desarrollan de cara a mejorar las prestación de VPLS. Sólo hace falta hojear un poco revistas especializadas para poder ver que no hay muchos adeptos.

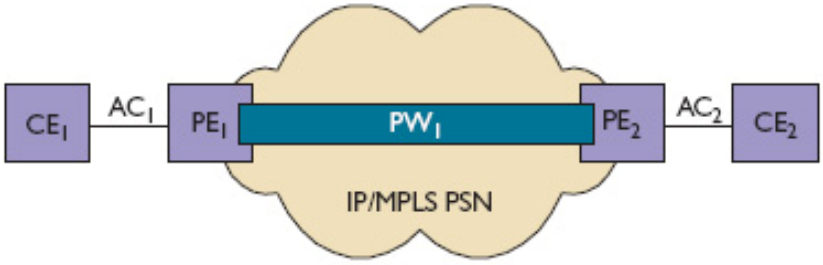


Fig. F.8 Ejemplo de red VPWS

El problema es que VPWS es una tecnología que trabaja punto-a-punto (como se representa en **Fig. F.8**), en un mundo donde las propuestas de las redes emuladas llevan la voz cantante. Es la fiebre de la denominada punto-a-nube, o lo que es lo mismo; una visión mucho más vaga de lo que hay más allá de los dispositivos frontera. Que, para que engañarnos, no es algo que debiera importar demasiado a los clientes que utilizan los servicios.

El entramado de conexiones o PWs necesita un surtido de procesos de gestión y mantenimiento para su correcto funcionamiento. Previamente es necesario definir una encapsulación tipo tanto para las pseudo-wires como para los túneles que atraviesan. También se requiere un plano de control para las gestiones de sesión y notificación de errores. Asimismo, y para garantizar el

dinamismo de la red, no están de más, capacidades de auto-descubrimiento. Por ejemplo, utilizando BGP (Border Gateway Protocol) o servidores RADIUS.

Además, y como ocurre en este tipo de ambientes, es necesario el desarrollo de capacidades de aprovisionamiento y operación, administración, y mantenimiento; dicho de otra manera, habilidades OAM. El *interworking*, o la habilidad de la red para soportar el uso de múltiples tecnologías entre puntos finales, es otro de los puntos destacados de investigación junto con estas capacidades-habilidades OAM.

Por último, en lo que respecta a la señalización, se barajan dos posibilidades: point-to-point y broadcast.

El primero requiere control directo de la sesiones entre los dispositivos frontera (PEs), para soportar el intercambio de control de datos. Y por su parte, el mecanismo broadcast se compagina con protocolo BGP, el cual permite un simple canal de control para enviar una copia de la información al resto de PEs.

Estos dos mecanismos son totalmente aplicables, sobretodo para aquellas redes totalmente malladas. La única condición es enviar la información a todos los puntos de la red. El problema llega cuando la red no es totalmente mallada, pues, la opción del broadcast deja de ser tan interesante.

F.4.3.2. VPLS

Tal y como ocurre con VPWS, en *Virtual Private LAN Services* (VPLS) se utilizan las PW para construir el entramado de la red del proveedor de servicios (PSN) (como se ilustra en **Fig. F.9**). Para ello, también hay que definir una serie de requisitos para que la red aparezca como una LAN para el usuario final. Algunos de estos requisitos pasan por el aprendizaje de direcciones origen MAC, la inundación de frames desconocidos, broadcast y unicast, o la definición del envío basado en direcciones MAC.

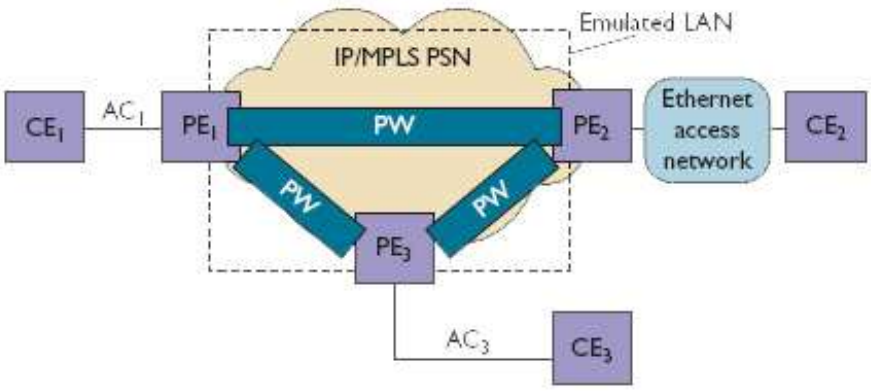


Fig. F.9 Ejemplo de red VPLS

Para poder conseguir la emulación de esta LAN, se dispone de un PE que hace de puente entre las diferentes CEs y la red central. De esta manera, la interfaz emulada aparece como un AC para los VPLS forwarding. Los cuales tienen establecida una conexión PW con el resto de VPLS forwarding.

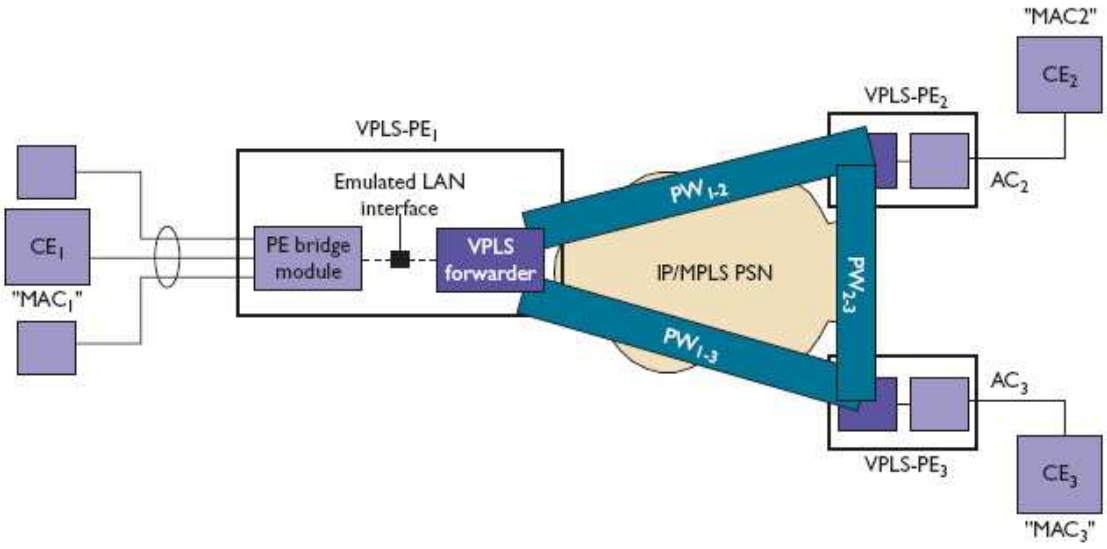


Fig. F.10 Ejemplo VPLS-PE

Estos VPLS forwarding o VSI (*Virtual Switching Interface*) tiene una gran importancia en el proceso de emulación LAN (ilustrado en **Fig. F.10**). Una de estas funciones es la de replicar y enviar frames en broadcast, multicast, unicast desconocido. Para ello, el VSI lee la dirección destino MAC del frame unicast recibido de la interfaz de emulación LAN. En el caso de que no contenga ninguna entrada en su tabla con la dirección de destino, replica el frame al resto de “forwarders” definidos en la red.

El punto clave del servicio VPLS es que las PW que interconectan las sedes VPN, deben utilizar una red totalmente mallada. Esto implica el uso de *split horizon* para evitar los bucles (*loops*), típicos de los envíos broadcast y de descubrimiento. Esto también implica la necesidad de utilizar *spanning tree protocol* dentro del IP/MPLS *core*.

F.5. L3VPN

Esta solución, es la preferida por los proveedores para crear sus redes de servicios. Concretamente es el BGP/MPLS IP VPN quien encabeza la lista de favoritos. Este un estándar del tipo PE-based, que complementa la versatilidad de MPLS con el mecanismo de gestión de direcciones de BGP. El resto de propuestas expuestas por el grupo de trabajo L3VPN de la IETF son los llamados VR (Virtual Router) IP VPN y el CE-based IPSec VPN. Dos soluciones más para el nivel predilecto de los proveedores.

Ya en la figura F.1 pudimos ver como el modelo L3VPN podía ser implementado tanto en PE-based como en CE-based. Pero la moda de los sistemas multipunto ha borrado de los documentos de investigación todo aquello que esté relacionado con CE-based para este nivel.

La verdad es que no me extraña porque durante la lectura de algunos de esos escritos he podido comprender la gran potencia de los mecanismos “basados en la red”. Aunque esto no quiere decir que desmerezca IPsec, porque es un sistema suficientemente contrastado (las grandes empresas lo utilizan para sus redes privadas virtuales), aunque poco tiene que hacer en la era del MPLS (a parte de unirse a él).

F.5.1. Desmenuzando L3VPN

Después de las numerosas descripciones que se han podido contemplar durante este anexo, llega un punto en que una mera descripción de los elementos es la mejor manera de hacer la descripción de un sistema. Desencajar todas las piezas como si de un puzzle se tratara, es lo que acto seguido se intentará hacer. Un resumen de los elementos y conceptos que son el alma de este sistema.

- La red del proveedor de servicios: Lo constituyen, los dispositivos P distribuidos en el corazón y en la frontera de la red (PE). La gran característica es que no dispone información alguna sobre las VPN que la atraviesan.

- Los dispositivos PE (Provider Edge): Son los nodos encargados de gestionar y mantener las bases de datos de las VPN y de su topología.

- Intercambio de rutas: Existen dos intercambios a destacar. El que se efectúa entre los CEs y PEs, y el realizado entre los PEs. El primero utiliza un protocolo de enrutado dinámico (por ejemplo BGP) para intercambiar las rutas VPN. El segundo también utiliza un protocolo dinámico para intercambiar las rutas VPN para poder enviar la información del cliente por la ruta correcta.

- Los túneles VPN: Son las autopistas de las VPNs de los clientes. Estas son creadas y gestionadas por los proveedores, y se utilizan para distribuir las VPNs de los clientes por la red sin que estos tengan conciencia de su existencia.

- CE-PE link: Conexión establecida entre estos dos elementos, para que CE pueda llegar a cualquier otro CE conectado a la red. Esta conexión es única en el caso del modelo PE-based, y múltiple (una conexión por CE) para el modelo CE-based.

Existen otros elementos en las redes L3VPN que tienen una gran influencia, pero estos forman parte de los modelos derivados de L3VPN.

Así y todo, se puede observar como las redes de este tipo son mucho más prácticas a los ojos de los clientes que las anteriores soluciones. Son muchos más simples para ellos. No deben establecer dispositivos específicos con personal muy especializado para controlar todas y cada una de las conexiones. Ni tener que "comprender y descubrir" la situación de los elementos que ella contiene.

Creo que con estos 5 puntos que acabamos de ver, podemos empezar a entender el porqué de su popularidad. Pero sigamos, no nos quedemos aquí y descubramos las diferentes soluciones que la representan.

F.5.2. PE-based vs CE-based VPN

Siempre una imagen vale más que mil palabras, y en este caso, las figuras siguientes (**Fig.F.11**, **Fig.F.12**) son también una ayuda irrefutable para entender los dos modelos de referencia VPN (PE-based VPN y CE-based VPN) interpretados para L3VPN.

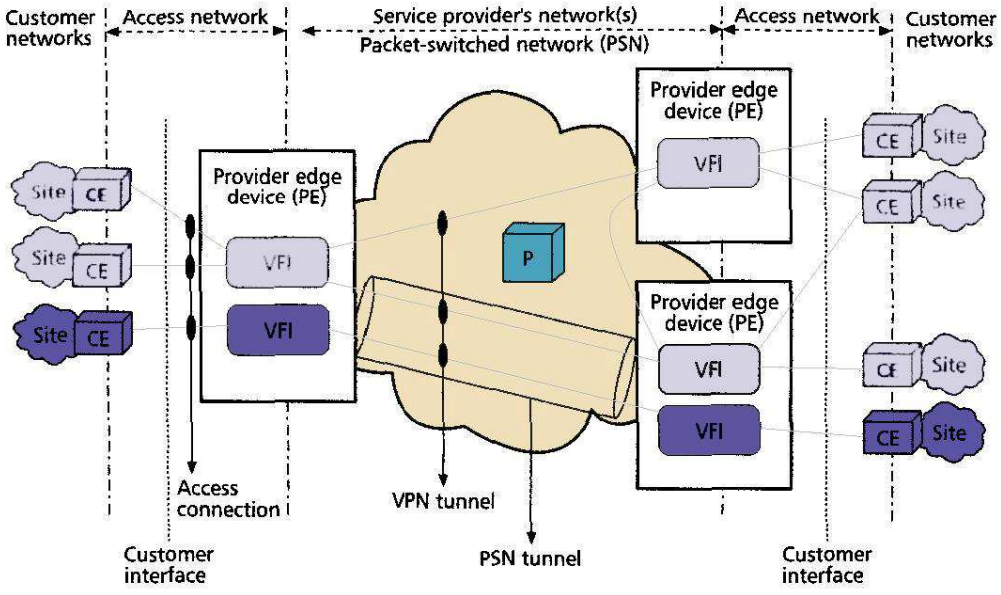


Fig. F.11 Modelo PE-based VPN

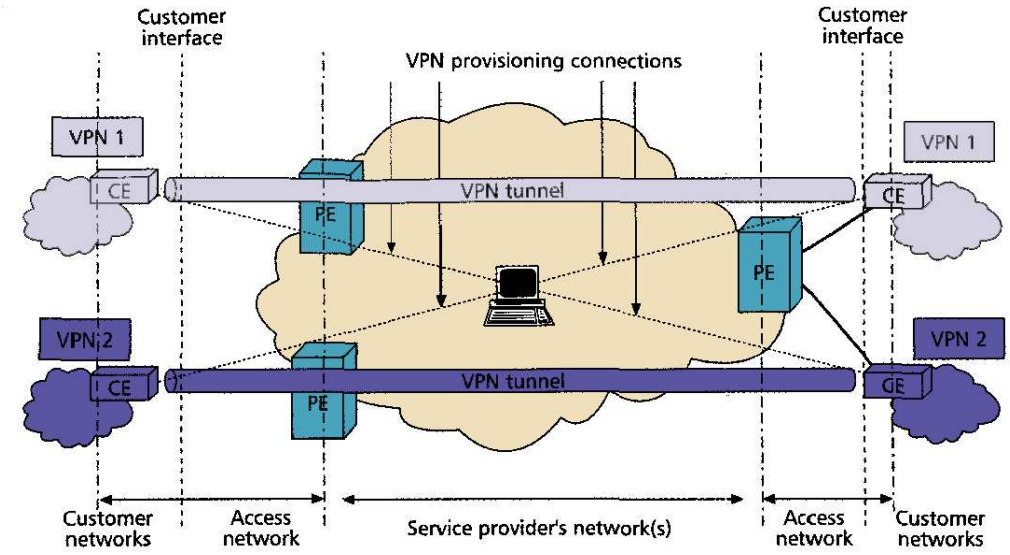


Fig. F.12 Modelo CE-based VPN

Son diversas las diferencias que se pueden observar entre estos dos modelos de referencia. Y a modo de resumen esquemático se podría decir que estos 4 puntos son los más significativos:

- Túneles VPN: En el caso del modelo CE-based los túneles atraviesan la red del proveedor y las redes de acceso para conectar los CEs. En cambio, en el modelo basado en la red, los túneles VPN se utilizan para unir los dispositivos PE.

- PEs: En los dos casos, estos elementos unen los dispositivos frontera de los clientes con la backbone. Pero la importancia que estos tienen en ambas soluciones es diferente. En el caso del modelo basado en la red, además de esta función de "puente", implementan funciones especiales vinculadas a las VPNs llamadas VFIs (*Virtual Forwarding Instantes*).

- CEs: De manera inversa, en el modelo CE-based, es en los dispositivos frontera de los clientes donde se implementan las funciones de las VPNs. Por otra parte, en CE-based, los dispositivos frontera de los clientes necesitan establecer una conexión por cada CE con el que quieran contactar, en cambio con PE-based sólo deben establecer una conexión con el PE.

- Responsabilidades: Es en la solución basada en la red donde la PSN tiene la responsabilidad de la configuración de las conexiones entre CEs. En CE-based estas responsabilidades recaen en los propios CEs.

Una de las cuestiones que pueden hacer decantar la balanza hacia uno o hacia otro, es sobretodo el precio de los dispositivos. El proveedor debe escoger

según el precio que quiera cobrar a sus clientes. En otras palabras; elegir si prefiere tener más o menos implicación en el desarrollo de las VPN o no.

Tener mayor implicación significa tener PEs mucho más sofisticados, más inteligentes y con muchas más preocupaciones. En resumen, PEs más caros. En cambio, si el proveedor decido no implementar la solución PE-based, traspasará el problema a los clientes que tendrán que invertir en dispositivos frontera más caros.

La respuesta a esta pregunta la tenemos en nuestras redes. El proveedor prefiere gastarse algo más de dinero en sus dispositivos frontera porque al fin y al cabo lo acabará amortizando. Podrá ofrecer precios más competitivos, y una oferta muy atractiva a sus clientes pues no deberían pagar un precio más elevado por su CE, ni el sueldo de alguien que lo supiera manipular.

F.5.3. PE-Based IP VPN

L3VPN tiene dos representantes del modelo basado en la red: el BGP/MPLS VPN y el VR. Ambos quedan reflejados en la figura F.13. En ella se muestran los distintos elementos y posibles protocolos que se pueden utilizar para los distintos procesos de descubrimiento, intercambio de direcciones, etc.

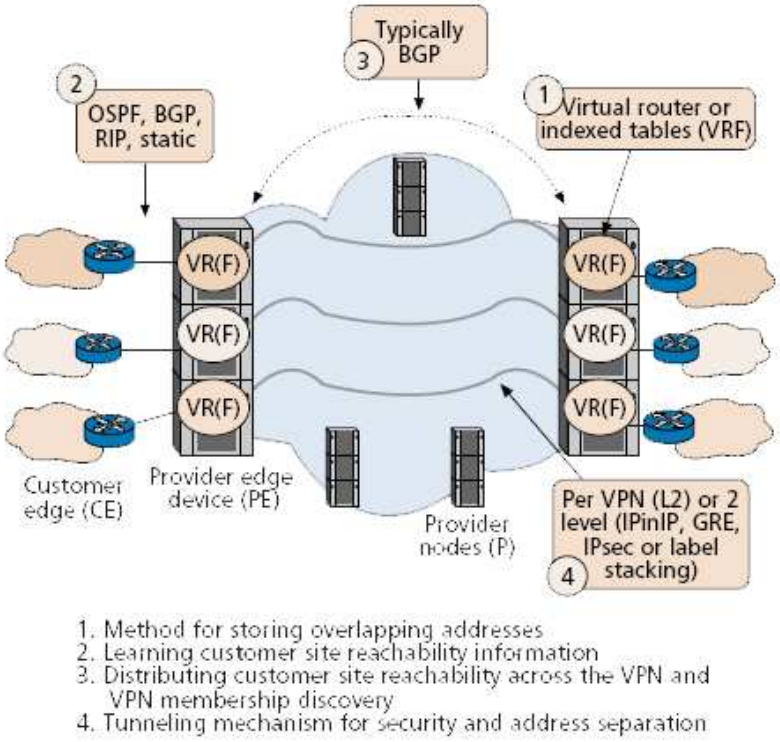


Fig. F.13 Ejemplo de L3VPN PE-based

Este modelo tiene la capacidad de guardar y mantener la separación entre espacios de direcciones de VPNs con múltiples clientes. Eso sí, para VR esta

configuración se realiza en los llamados VR, creados para cada VPN. Y en el caso del 2547bis, se crea en las tablas VRF.

Ambas opciones también soportan la creación de túneles entre PEs o VRs y la utilización de BGP para el descubrimiento de puntos finales en las VPNs. En realidad no hay demasiados puntos en que diverjan, aunque uno de los más importantes se encuentra en la definición de los protocolos de *tunneling*. En el caso de VR, se puede utilizar cualquier tipo (incluso circuitos ATM y FR), pero para el 2547bis sólo se definen MPLS y *tunneling* basados en IP.

Hechos estos apuntes, ya podemos pasar a explorar cada uno de ellos por separado. ¿Empezamos?

F.5.3.1. BGP/MPLS IP VPN

BGP/MPLS IP VPN es como se conoce al RFC 2547bis, extensión del RFC 2547. Esta solución se constituye por la simbiosis de dos tecnologías como son MPLS y BGP. Se complementan para que los paquetes que deben atravesar la red puedan llegar a su destino, teniendo actualizadas las rutas y con el mínimo esfuerzo por parte de la red.

Pero como es lógico, esta solución no se compone única y exclusivamente de estas dos tecnologías si no que comparten protagonismo con otros componentes y protocolos:

- *VPN routing and forwarding* (VRF) *instance*: Estas instancias son asignadas a cada VPN conectada. Cada PE las mantiene separadas una de las otras, y actualiza sus rutas con el CE manualmente o a través de un protocolo de enrutado.

- VPN IPv4: Es un sistema de dirección extendida con el que la red evita los problemas de duplicación de direcciones. Con ello, dos o más clientes pueden utilizar el mismo rango de direcciones sin temor a fallos en el envío de paquetes por la red.
  Como se puede observar en **Fig. F.14**, se añade un identificador interno llamado RD (Router Distinguisher) de 64 bits a los 32 de una dirección IPv4. Con ello los PE se configuran con un RD distinto por cada por cada VRF o instancia conectada al VRF.

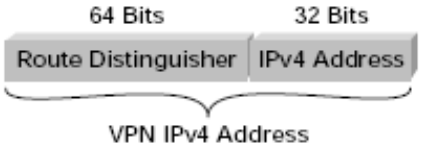


Fig. F.14 Representación de la dirección de VPN IPv4

- RT: El *Route Target* son unos identificadores creados por el MP-BGP para marcar grupos de VRF de una VPN específica. Los PE marcan las rutas enviadas con este identificador, de esta manera los PE que

reciben estas rutas actualizan la VRF especifica con esa RT. Si no poseen ninguna VRF etiquetada con ese RT especifico, descartan la información recibida.

- MP-BGP: El multiprotocolo BGP es una extensión de BGP, con el que los PE distribuyen sus rutas VPN a otras PEs de la red. Estas rutas son intercambiadas por el "core" de la red, sin que los Ps tengan ningún conocimiento de la información que se envía.

- *MPLS label*: Se utiliza para identificar y separar el tráfico dentro de un túnel que pertenece a VPN en particular. Cada ruta es asociada con esta etiqueta, y cuando esta ruta es propagada por el protocolo BGP, esta etiqueta es propagada con ella.

Como se puede deducir de esta serie de componentes y protocolos, todos los paquetes que viajan por la backbone son etiquetados con la MPLS label. Por ello podemos decir que los paquetes que viajan por el interior de la red son paquetes MPLS. De todas formas, los clientes no tienen la necesidad de adaptar sus CEs para poder trabajar con MPLS. Son las PEs las que se encargan de todo. Los CEs reciben y envían a la red de servicios paquetes IPv4 sin ningún tipo de florituras.

También se les otorga cierta libertad a los proveedores de servicios pues, no es necesario que los routers PEs utilicen el mecanismo de túnel de MPLS. En realidad pueden utilizar GRE o IPsec.

Este es un modelo que otorga toda la inteligencia a los extremos. Concretamente, asigna las responsabilidades a los dispositivos PE, que etiquetan, clasifican y vinculan los paquetes y las rutas que intercambia con los CEs y pertinentes PEs. Los P, no son conscientes de las VPN, no trabajan con MP-BGP. Sólo leen las etiquetas MPLS para encaminar los paquetes correctamente. Trabajo en equipo.

F.5.3.2. Virtual Router

Esta propuesta coge el nombre de su principal elemento: el router virtual. Este VR proporciona todas las capacidades de un router real, pero en realidad sólo emula sus funciones. Los VR se sitúan en los PEs, ya sea de manera individual o colectiva. Ahí, representan a distintas VPNs que mantienen las tablas de enrutado independientemente de los procesos del resto de VRs de la PE. Como las tablas permanecen independientes un de las otras, las direcciones pueden ser las mismas para dos o más VPNs.

Para el dispositivo frontera del cliente, la VR aparece como un router real con el que intercambia la información de enrutado. Cosa que no dista de cualquiera de las otras opciones para las backbones. Pero en cambio, existen dos puntos de los que dista de su hermano BGP/MPLS. El primero de ellos es el mecanismo de intercambio de las rutas.

En el RFC 2547bis recordemos que las enviaba utilizando MP-BGP como vía de transporte. En cambio en VR VPN el intercambio entre VRs se produce creando túneles al margen de los creados por la PSN. Para ello, se puede utilizar cirtuitos de FR o ATM, y también IPsec, IP-in-IP o GRE; incluso MPLS.
Este es un punto a favor de la arquitectura basada en los VR ya que si hubiera algún problema con las sesiones de BGP, podría afectar a la conectividad de los servicios a los clientes.

Por otra parte, en el RFC 2547 se especifica que es necesaria la creación de una simple malla de túneles entre los PE. En cambio, en la arquitectura VR es necesario mantener separados los túneles de cada VPN. De manera que, cada VR debe tener creado un túnel por cada VR de esa misma VPN. Esto representa un gran esfuerzo de configuración de un número de VPN que puede incluso ser prohibitivo.

Esta última es una de las razones por la muchos investigadores se inclinan por BGP/MPLS VPN. De todas maneras, muchos no consideran que la solución basada en VRs no tenga futuro, ya que es también una buena alternativa, aunque por lo visto, menos atractiva para los proveedores de servicios. Ya se verá en un futuro, si VR desbanca a BGP/MPLS o no.

F.5.4. IPsec-Based L3VPN

IPsec-based L3VPN es la última de las grandes propuestas que se describirán. Esta es tal vez la menos definida, ya que aún hoy se siguen retocando ciertos puntos, sobretodo en cuanto a seguridad y propagación de rutas se refiere.

Esta solución interconecta dispositivos CE pertenecientes a varios clientes vía Internet. Estas conexiones pueden ser construidas y mantenidas tanto por los clientes como por los proveedores, ya que es una herramienta muy sencilla.

El alma de esta solución es IPsec que proporciona alguno de los servicios de seguridad más perseguidos hoy en día: confidencialidad e integridad de datos, autenticación del origen de los datos y anti-copia.

IPsec de todas formas, también define algunos nuevos formatos de paquetes, tales como la ESP (*Encapsulating Security Payload*), para la confidencialidad. ESP por su banda, soporta cualquier tipo de encriptación simétrica, incluyendo el estándar de 56 bits ESP o el Triple DES (3DES), y el AES (*Advanced Encryption Standard*).

También cabe añadir que los parámetros son comunicados y negociados entre dispositivos de red con el uso del protocolo IKE (*Internet Key Exchange*).

Por lo que se ha podido observar, la seguridad es uno de sus puntos fuerte; que debemos asociar con la gran flexibilidad para el uso de distintas

tecnologías de transporte (Internet, MPLS-based networks, backbones IP), hacen de esta, una solución atractiva.

Esta supera en aspectos de seguridad a la solución basada en MPLS, y no ha faltado tiempo para que empresas como Cisco hagan sus propuestas de unión de las dos tecnologías: Network-based IPsec VPN ("*Comparing MPLS-Based VPNs, IPSec-Based VPNs, and a Combined Approach from Cisco Systems* "; Cisco Systems, Inc.). Esta puede ser una buena opción para complementar la tecnología MPLS en el "core", y otorgar de más seguridad a lugares de la red olvidados como la frontera de la red y el exterior de esta.

ANEXO G. MPLS. LA OTRA CARA.

En este anexo, se exponen las razones por las que en estos momentos existe un debate con MPLS como protagonista. Me refiero a que si MPLS no hubiese sido suficientemente adecuado para las exigencias del mercado, o al menos, si no hubiese sido la mejor de todas las propuestas, MPLS no podría entrar en ningún tipo de debate.

Las características y los beneficios que aporta MPLS, y sobretodo su conjunción con VPN, va más allá de todo lo que se expone el resto del trabajo. Exponerlo todo, y explicar al pie de la letra las razones de cada punto, significaría expandir muchísimo este trabajo. Y no sería adecuado ya que tampoco es una parte sumamente imprescindible.

Así pues, a modo de resumen, durante este anexo se expondrán los beneficios que aporta MPLS basado en VPN respecto a otras tecnologías (sobretodo IP/ATM). Sin olvidar un apartado importante respecto a las mejoras y al "techo" de esta tecnología. Me refiero a las propuestas de futuro y a su futuro en general en nuestras redes.

G.1. Características de MPLS

En sus días de gloria, ATM era la respuesta a las demandas de aquellas aplicaciones con requerimientos de garantías de tráfico. Fue en todo caso, una aproximación que ayudó a la integración de estos flujos, en una red con grandes carencias. Pero, para muchos una solución que dejaba mucho que desear. Un puro trámite, a la espera de algo mejor.

Se necesitaba una tecnología con la que poden ofrecer Calidad de servicio (QoS) y garantías extremo a extremo, en redes tan inseguras y poco efectivas como Internet. El *Best Effort* no beneficiaba a la expansión de una propuesta que cada día ganaba más fuerza: "la convergencia de servicios".

MPLS es actualmente una solución lo suficientemente consistente como para ofrecer Calidad de servicio y garantías de servicio extremo-a-extremo. A parte de eso, aporta a la red más velocidad en las gestiones con los paquetes, más robustez y versatilidad, entre muchas cosas.

Estas características, y aquellas que se expondrán en el G.2, no podrían existir sin el carro de elementos y protocolos que componen la tecnología MPLS.
Entre todos ellos, he escogido 4. Dos de ellos ya los conocemos, pero los dos últimos será la primera vez que se mencionarán.

G.1.1. El uso de etiquetas

Las etiquetas son el buque insignia de MPLS. Sin duda alguna, esta es una de las características más importantes y la que aporta muchas de las ventajas respecto otras soluciones.

La utilización de etiquetas proporciona estas ventajas en comparación con ATM:

- Integración: Permite soportar servicios como ATM, FR, etc., sin que eso suponga un cambio en los dispositivos del cliente. Ya que el LSR frontera se encargará de etiquetar el paquete-frame, y etiquetarlo como MPLS.

- Mayor Fiabilidad: En las infraestructuras ATM se requiere la creación de una malla de PVCs. Si se produjera fallo en alguna de las conexiones, esto provocaría la actualización del enrutado red, lo que podría suponer la perdida de otras conexiones.

- Mejor Eficiencia: En un ambiente IP, los PVCs son vistos como conexiones de un único salto. Esto puede confundir y crear ineficiencias, por la mala elección del camino óptimo.

- CoS: MPLS puede ofrecer CoS (Clases de servicio) sin tener que añadir protocolos adicionales, como en el caso de ATM.

- Escalabilidad y manejabilidad de las VPNs: La información y la gestión de las VPNs se tratan a lo largo de la frontera de la red. Unidos a BGP, otorga, a parte de escalabilidad y manejabilidad, una fácil gestión y creación sencilla de socios de VPN (memberships).

- Más robustez: Como la inteligencia se traslada a los dispositivos frontera, el *core* de la red puede despachar paquetes mucho más rápido. Esto ayuda a evitar el descarte de paquetes por congestión y los retardos excesivos.

- Ingeniería de Tráfico: Esta propiedad impide la sobreutilización y la infrautilización de nodos de la red. Ya que esto puede provocar congestión en la red, pero sobretodo, poca eficiencia.

G.1.2. Estructura

Por mucho que exista un etiquetaje, la estructura de la red es una parte fundamental ya que, en parte, acaba determinado el funcionamiento de la misma.

En el caso de MPLS, se pueden distinguir sobretodo cuatro elementos:

- CE (Customer Edge): Como se puede observar en la figura (**Fig. G.1**), es el dispositivo frontera de la red del cliente. Gracias al valor de integración que aporta el uso de etiquetas, este dispositivo no necesita conocer todos los elementos de la red, ni utilizar MPLS.

- PE (Provider Edge): El LSR frontera trabaja como elemento puente entre la red del cliente y la *backbone*. Es el punto donde se lee la cabecera del paquete que entra y se etiqueta según su destino, las preferencias de CoS del cliente, la VPN a la que pertenece, y otros elementos distintivos. Si el paquete sale, este router debe eliminar la o las etiquetas que se hayan añadido al paquete, para acto seguido encaminarlo al CE destino.

- Core Network: Como son los PEs los encargados de la inteligencia de la red, los Ps (Providers) o nodos del core, deben leer la etiqueta e encaminarla convenientemente. Esta ligereza, ayuda a que puedan tratarse los paquetes de manera más individualizada al poder ejecutar con mayor plenitud una ingeniería de tráfico que se adapte al tiempo.

- LDP (label Distribution Protocol): Este es el protocolo encargado de la distribución de la información de la etiquetas entre dispositivos. Para esta tarea, puede asociarse con el BGP.

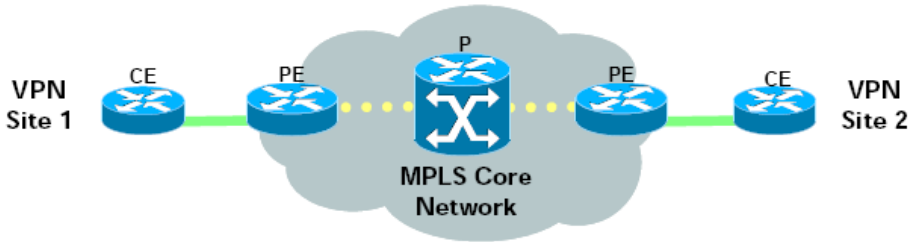


Fig. G.1 Estructura de la red

G.1.3. Aplicaciones

La diversidad de servicios con los que puede trabajar, y las tecnologías que puede soportar, propicia que existan una gran cantidad de aplicaciones en las que se puede involucrar. Entre ellas:

- Ingeniería de Tráfico
- Integración de IP con: ATM, Frame Relay, SONET/SDH, Ethernet, redes ópticas
- VPN (con protocolos como BGP)
- Diferenciación de niveles de servicio (CoS)
- Soporte multiprotocolo

De entre estas aplicaciones, la diferenciación de niveles de servicio y una buena ingeniería de tráfico ayudan a conseguir el objetivo de proporcionar QoS y eficiencia en redes compartidas. Con esta presentación, son muchas las propuestas nuevas que pueden surgir ya que se dispone de la tecnología adecuada, y de niveles de servicio elevados.

G.1.4. Protección contra fallos

Si una red quiere ofrecer la máxima eficiencia y robustez a sus clientes, una buena gestión de los fallos de las conexiones ayuda a solventarlo. Hay que tener en cuenta que es imposible evitar que se produzcan desconexiones en la red. En cualquier momento puede un operario de una obra cortar una fibra, o que le caiga un rayo a alguno de los elementos de la red. Por eso, lo único que se puede hacer es intentar minimizar los riesgos de desconexión y restablecer rápidamente el servicio.

Con ese objetivo, existen métodos de protección que siguen un ciclo que va desde la detección de un fallo en un camino de datos, hasta que el tráfico puede reestablecerse en este camino. Este ciclo involucra a varios componentes: un método de encaminamiento que selecciona caminos de trabajo y de respaldo; un método de reserva de ancho de banda en ambos caminos; un método de señalización para configurar (distribuir las etiquetas) en los caminos de trabajo y respaldo (o protección); un mecanismo de detección y otro de notificación de fallos, necesarios para indicar al nodo responsable de tomar las acciones de respuesta al fallo que se ha producido; y, finalmente, un mecanismo para desviar el tráfico desde el camino de trabajo (en el que se ha producido el fallo) hasta el camino de respaldo (acción de *switchover*). Opcionalmente, podemos disponer de un mecanismo de detección de la recuperación del camino original (posiblemente considerado el camino más óptimo) y de los elementos necesarios para volver a restablecer el tráfico.

Un aspecto que distingue a MPLS de otros mecanismos de protección es que podemos aplicar protección a diferentes niveles. En los dominios MPLS, podemos disponer de mecanismos de protección para todo el camino o bien para un segmento de éste.

De esta manera, y como se muestra en la figura (**Fig. G.2**), MPLS posee tres mecanismos a disponibilidad del proveedor:

- Mecanismo de protección global: Es aquel que abarca de extremo a extremo de la red de servicios. Las acciones de protección se gestionan desde el nodo de ingreso. En caso de tener que utilizar el camino o el cable o la fibra de protección, tendría como punto final el mismo nodo de salida que en el otro caso.

- Mecanismo de protección local: El dominio de este mecanismo se reduce al tramo o tramos del camino que han caído. En este caso, la protección se activa en el nodo donde se produce el fallo; lo que hace

que sea mucha más rápida la restauración de la comunicación. En lo que respecta al camino de protección, tendrá que existir un segmento de protección por cada segmento a proteger. Una desventaja respecto a la anterior alternativa.

- Mecanismo de protección inversa: La idea principal de esta solución es la de devolver el tráfico al nodo de ingreso, para evitar la pérdida de paquetes. Es más lento incluso que el mecanismo global pero disminuye la pérdida de paquetes y por lo tanto, el número de notificaciones de fallos-pérdidas.

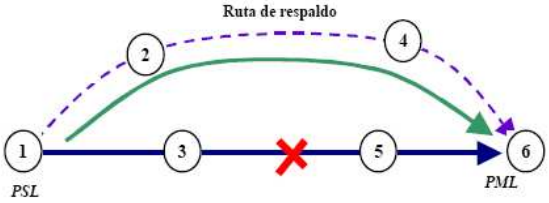


Fig 2.a Mecanismo de protección Global

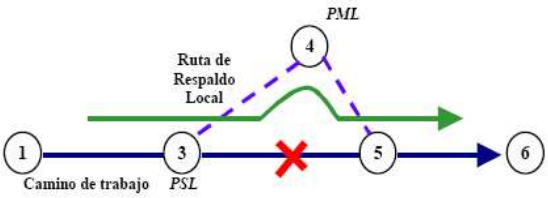


Fig 2.b Mecanismo de protección Local

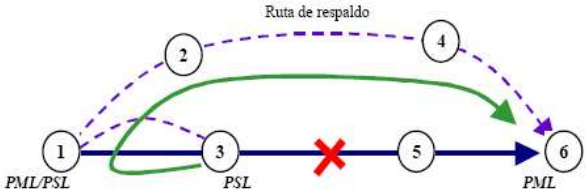


Fig. G.2 Mecanismos de protección

El buen nivel de protección ante fallos que ofrece MPLS ayuda a cumplir los requisitos de QoS. Este nivel, supera con creces al de otras tecnologías como por ejemplo Ethernet (que tarda de 30 segundos a varios minutos en su recuperación). En cuanto a MPLS, se puede conseguir la recuperación en no más de 50 ms. Un tiempo que ayuda a evitar incumplimientos de los contratos de QoS establecidos con los clientes.

G.2. Beneficios de VPN/MPLS

MPLS no sería nada sin VPN. VPN no sería nada sin MPLS.
Se puede tomar como algo exagerado este comentario, porque por sí mismas, ya son tecnologías con grandes puntos a favor.

Sin embargo, la gran eclosión de MPLS comenzó al unirse al grupo de soluciones beneficiarias de las redes virtuales. Y VPN, aunque tenía una larga historia tras sus pasos, con ATM no acabó de cuajar, ya que ATM no acaba de aportar los niveles de QoS, eficiencia y robustez que tanto se reclamaban. Con MPLS, como se podrá ver a continuación, por fin ha conseguido encontrar a su media naranja.

Veamos pues los beneficios que presenta VPN/MPLS:

- Integración:
  - Sencilla con clientes de intranets
  - No se requiere el soporte de MPLS por parte de los clientes, ni de cambios en la intranet
- Escalabilidad:
  - Posibilidad de soportar miles de “sites” por VPN y centenares de miles de VPNs por proveedor de servicio
  - Los routers P no mantienen ninguna información de rutas de las VPN, lo que incrementa la escalabilidad y evita cuellos de botella
  - La incorporación de un nuevo cliente, sólo supone configurar la entrada en el PE, no la re-configuración de todos los elementos involucrados como en ATM
  - Los clientes no deben preocuparse por la duplicidad de direcciones. Por lo tanto no es necesario el uso de NAT, excepto en el caso de duplicidad en la misma VPN
- CoS:
  - Soporta múltiples clases de servicios
  - El cliente elige las clases de servicios que quiere para sus envíos, y éstas se implementan por parte del proveedor o ambos
  - Se pueden definir distintas políticas de actuación como la probabilidad de descarte o el retardo
- Simplicidad de uso:
  - Las VPNs las gestiona el proveedor de servicios
  - Soporte transparente para direcciones IP privadas
  - Múltiples clases de QoS para implementar las exigencias de la empresa
- Bajo coste:
  - Independencia de los equipos del cliente al servicio
  - La implementación de la VPN no requiere un hardware específico ni costoso para ser instalado
  - Se pueden integrar distintos servicios y aplicaciones sobre una misma plataforma: voz, datos y video

- Independencia:

  - Una VPN puede soportar distintos protocolos de acceso/transporte: dial, xDSL, ATM, etc.
  - El servicio de envío es independiente de la tecnología de transporte o de acceso

- Rápida recuperación a fallos de conexiones

- Seguridad:

  - No es necesario el uso de protocolos o aplicaciones adicionales para soportar niveles de seguridad comparables a ATM
  - Los tráficos VPN se mantienen separados
  - La distribución de rutas VPN se restringe sólo a los miembros de la propia VPN

Considero que estos son los beneficios más importantes de esta unión. Evidentemente, es mi pequeña síntesis de lo que se puede explicar en un sinfín de páginas. Pero aporta la suficiente información como para poder ver el poder integrador de esta unión, y el abanico de posibilidades que se abren para la aparición de nuevas aplicaciones-servicios.

G.3. Propuestas

Son muchas las propuestas que se pueden encontrar. Desde la integración total de ATM en ambientes MPLS, como la incorporación de nuevos elementos en la red para poder incrementar la fiabilidad en las interfaces de Internet.

De entre todas ellas, como llevo haciendo a lo largo del TFC, sólo he escogido las más interesantes. Lo he hecho teniendo en cuenta dos puntos: que haya encontrado la propuesta en documentos de autores y compañías diferentes, y que encuentre que puede dar mucho que hablar.

Dicho esto, estos son simplemente los tres ejemplos de las propuestas que hay en el mercado. Unas propuestas que aún están madurando, pero que ofrecen una idea de lo que puede llegar en un futuro no muy lejano.

- Ethernet/MPLS: Los ambientes que envuelven Ethernet, ven claro el siguiente paso. Consideran que Ethernet ha llegado a la madurez como infraestructura de red y que MPLS puede eliminar las carencias que presenta: ingeniería de tráfico, recuperación de fallos, escalabilidad de servicios, convergencia de servicios con QoS.
  Con ello conseguirían llegar hasta ámbitos metropolitanos con suficiente solvencia y velocidades de 10 Gigabits (y en aumento)

- GMPLS (*Generarilized Multiprotocol Label Switching*) y MPλS (*Multiprotocol Lambda Switching*): Estas son dos de las soluciones que se manejan para la integración de MPLS en ámbitos ópticos. Con ello, se conseguiría integrar los beneficios de la conmutación de etiquetas a conmutación de Lambdas, permitiendo soportar características poco agraciadas en conmutación de paquetes. De esta manera se daría un paso más hacia la interoperatividad de redes y servicios.

- Network-based IPsec VPN: Esta es una propuesta bautizada por Cisco, pero considerada por la mayoría de autores como una gran aproximación a un nivel de seguridad cercano a lo deseado.
  Con la tecnología IPsec, MPLS basado en VPN puede garantizar la seguridad a puntos de la red donde tiene pequeñas carencias: en la frontera, fuera de la red y ambientes locales.